INDEX

1 PACKET SWITCHING

1.1 LEARNING OBJECTIVES

- Switching techniques
- Circuit Switched Sub-Networks
- Store And Forward Switched Sub-Networks
- Packet Switching
- Datagrams And Virtual Circuits
- Virtual Circuit Routing

1.2 INTRODUCTION

A distributed computing system consists of end systems interconnected through interconnection subsystem (also called sub-network) as shown in the Fig. 1. The sub-network can provide fixed connections as the case of dedicated links between the end systems else it may provide switched interconnection service on request from end systems. In this chapter we shall briefly discuss the switching techniques used in the switched data sub-networks.

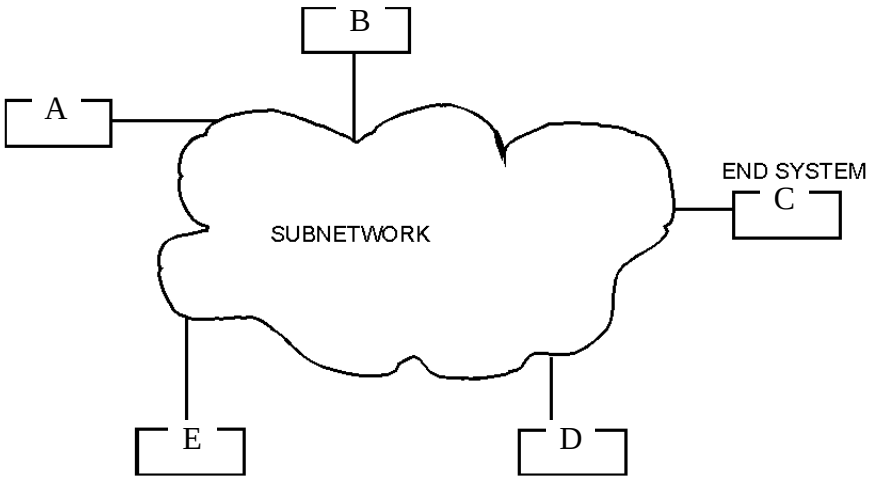


Figure 1: **Sub-network**

1.3 SUB NETWORK TOPOLOGY

Switching is the selection and establishment of a path from a source to a specific destination through the sub-network. Switching is carried out on specific demand from the source. The motivation for resorting to switched networks arises out of the following two major requirements:

1.3.1 Flexible Topology

Switching provides capability to deliver information presented at one access point of the sub-network to a variety of destinations, which can be selected by the users. Thus, switching provides a flexible interconnection topology.

1.3.2 Resource Sharing

The sub-network resources are available to all the users of the sub-network. Thus, the interconnection resources are shared by many users.

A switched data sub-network consists of an interconnected collection of nodes. The node interconnecting links are called trunks (Fig. 2). Data is transmitted from source to destination by being routed through these nodes. For example, data from end system an intended for F is sent to the entry node 4, switched to node 5 and then to node 6. Node 6 is exit node as end-system F is connected to it. Each end system is identified by a unique address to facilitate routing the call to the destination.

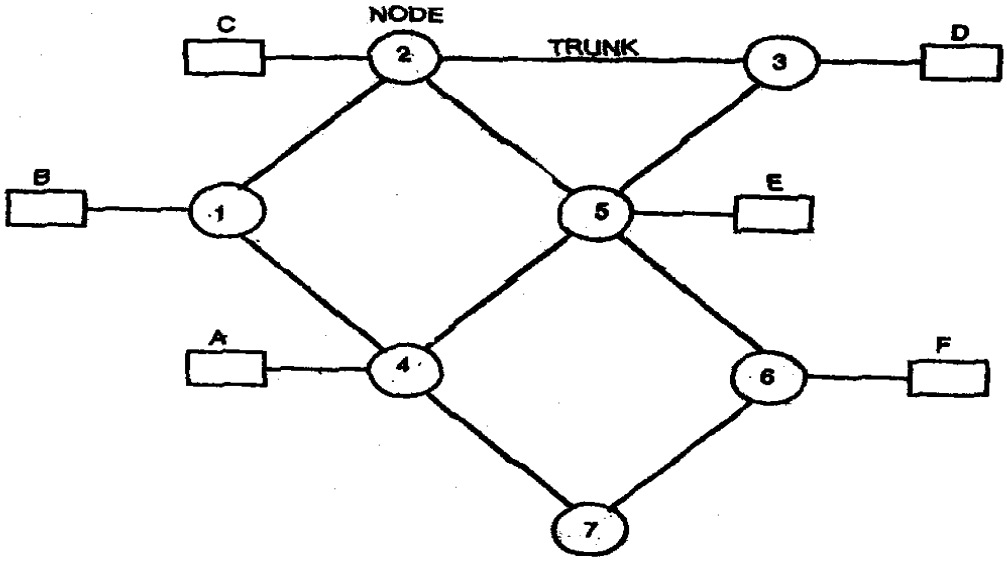


Figure 2: **Trunks**

1.4 SWITCHING TECHNIQUES

At each node, there is a need to decide the route through trunk circuits which finally lead to the exit node. This switching function and other related functions are carried out at the nodes. There are two basic techniques employed in the nodes for switching data to appropriate route:

- Circuit switching
- Store-and-forward switching

1.4.1 Circuit Switched Sub-Networks

In circuit switched sub-networks, a connection between the two communicating end systems is established and then transmission of data takes place on this connection. The sub-network consists of circuit switching nodes which are interconnected by trunk circuits. A node connects incoming circuits to an outgoing trunk circuit. The most common example of circuit sub-network is the telephone network. Trunks may be real (metallic pairs, FDM channels, PCM channels) or "virtual". If they are virtual, they must be immediately available to their user whenever information is to be transmitted.

A connection is built up by connecting the trunk circuits in tandem up to the exit node. To establish this connection, the originating station sends a CONNECTION ESTABLISHMENT REQUEST with address of the destination to the entry node. The entry node builds up a path by connecting one of the trunk circuits going in the desired direction to the end system (Fig. 3). The address information is transferred to the next node where again cross connections are made. This process is repeated at each intermediate node and finally at the exit node which connects to the destination. The exit node signals INCOMING CALL INDICATION to it. If the destination returns a CALL ACCEPTANCE signal, the sub-network sends CONNECTION CONFIRMATION to the call originator. Thus, an end to end connection is established. After the confirmation is received, data transfer can begin on the established connection. The connection is bi-directional, i.e. transmission can be either direction. The users have full time ownership of the connection till it is released by them. Note that address of the destination is specified only once during the call set up. All subsequent data blocks are transmitted on the path already established

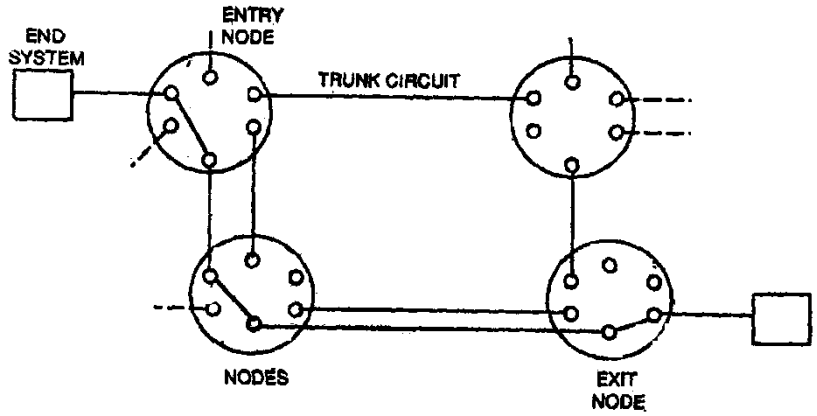


Figure 3: **Connection Establishment**

The sub-network usually does not retain the information on the end-points of a connection after it is established. Therefore, if the connection gets broken, the sub-network does not have any capability to restore the connection.

The circuit switched sub-network provides end-to-end connection for transmission of data and it does not have any error control or flow control capabilities. Fig. 4 shows the layered model of a connection through circuit switched sub-network. Note that the connection does not involve layers 2 and 2 of the sub-network node for transfer of user data. Relaying function of layer 1 must be utilized for transmission of the electrical signals. In other words, the sub-network does not incorporate error and flow control functions for the user data.

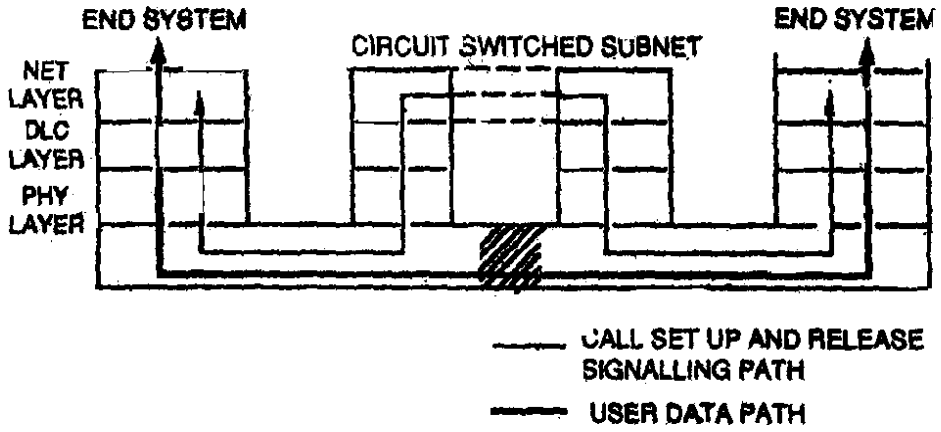
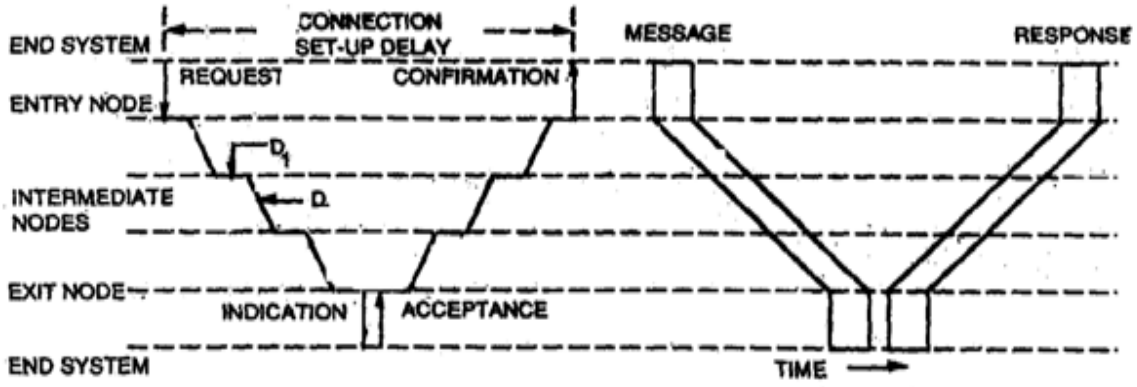


Figure 4: **Layered Model of Connection**

1.4.2 Delays In Circuit Switched Sub-Network

Connection establishment in circuit switched sub-networks involves certain set up as shown in Fig.5. It includes cross connection establishment delays at each node and connection request propagation delays. Once the connection is set up, user data transfer involves only propagation delay and it is constant. There is almost no delay at the nodes during data transfer phase. Data is transmitted immediately and incrementally as soon as



D_1 Node Processing Delay D_2 Node-to-Node Propagation Delay

Figure 5: **Delays in circuit switching**

it is presented to the sub-network. During the user data transfer phase, the delivery delay from source to sink is constant as all the data blocks are transmitted on the same path through the sub-network. Therefore, time relationships of data blocks and their sequence of transmission are maintained. If "A" is transmitted t seconds before "B", "A" is delivered t seconds before "B" at the other end.

During peak hours of traffic, once a connection is established, there is no increase in transmission delay through the sub-network as a dedicated transmission path always exists. There may be increased delay in establishment of the connection as network resources may not be free.

In the next section, we shall study another switching technique called store-&-forward switching. Basic features of these two switching techniques, circuit switching and store-&-forward switching, are summarized in Table 1 given at the end of next section.

1.5 STORE AND FORWARD SWITCHED SUB-NETWORKS

Store-and-forward sub-networks can be of two types:

- Message switching sub-networks.
- Packet switching sub-networks.

In message switching sub-networks, the complete message is switched at the sub-network nodes. In packet switching sub-networks, the message is first divided into smaller packets of data and then these packets are switched through the sub-network. The switching mode adopted in both these sub-network types is store-&-forward mechanism described below.

Store-and-forward sub-network consists of store-and-forward nodes interconnected by trunks. One channel is usually sufficient between a pair of nodes. Multiple channels can be provided to increase reliability. Each node is equipped with a storage device wherein all incoming messages are temporarily stored for onward transmission. The basic operation of store-and-forward service is similar to the telegram service. A message along with an address is sent from node to node till it reaches its destination.

To understand the basic operation of the store-and-forward switching mechanism, let us say the end system. 'A' wants to send a message to end-system 'B' (Fig. 6). End system 'A' sends its message along with the address of the destination and its own address to the entry node 1 .

Node 1 accepts the message, analyses the address and puts it in a queue of messages awaiting further transmission. At each node, a routing table is maintained. It contains entries indicating destination nodes and the corresponding outgoing trunks from the node.

There is a separate queue for each trunk. Since the destination node may be accessible via more than one route, decision to send the message to a particular next node shall depend on the expected delay in its queue. Let us say, the message from A is sent to node 2. The message received at node 2 is again put in a queue of messages awaiting transmission to node 4. When its turn comes, the message is sent to node 4 which delivers it to the destination.

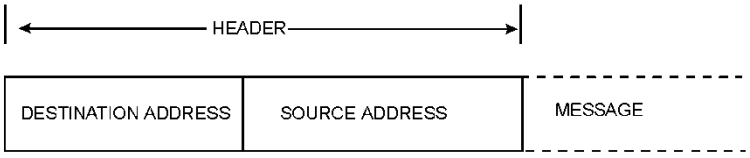


Figure 6: **Header**

The store-and-forward service is unidirectional. After delivery of the message, the sub-network does not send back any confirmation to the source. If end-system B is required to send an acknowledgement to the message received from A, the acknowledgement will be treated as like any other message by the sub-network and will carry the address of A in its header. It is not so in circuit switching service which provides an end-to-end connection between two communicating devices for communication in both the directions.

For node-to-node transfer of the message, the sub-network may employ some error control mechanism. The message may be appended with error checking bits and if any error is detected by the receiving node, it may request the sending node for re-transmission of the message. Therefore, the sending node is required to keep a copy of the message till an acknowledgement is received. Once a node has correctly sent a message, it discards the copy and thereafter it has nothing to do with the message.

Since at each stage of transmission, a message is stored in a buffer at the node, each node-to-node transfer is an independent operation. The trunks can operate at different data rates. Even the source and sinks of the messages can operate at different speeds. It is not so in circuit switching where the users have to operate at the same speed.

Note that in store-and-forward switching, there is no call establishment phase. Each block of information is treated as independent entity by the sub-network and, therefore, each block of information carries the destination address. Thus, unlike circuit switching where address was sent only once during call establishment phase, in store-and-forward switching, address is repeated on each block of information.

1.5.1 Delay In Message Delivery

Fig. 7 shows the timing diagram of a message being transmitted through a store-and-forward sub-network. The message passes through the entry node, two transit nodes and then the exit node to arrive at the destination.

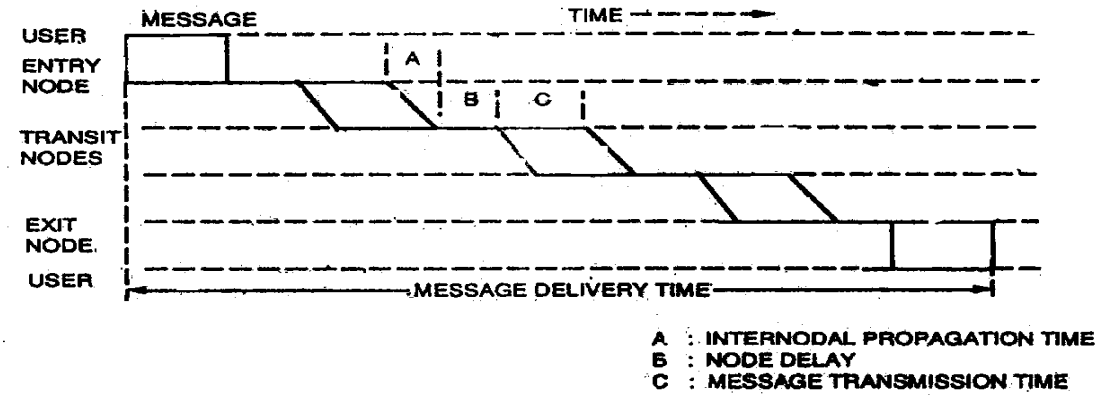


Figure 7: **Timing Diagram of message**

Message delivery time is sum of the following components:

- Time required to send the message to the entry node. It is determined by the transmission data rate and message size. Propagation time to the entry node is usually negligible.
- Node delay which includes :
  - Message processing at each node (time required for error checking, routing, etc.).
  - Waiting time in the queues at each node.
- Transmission time at each node (determined by the transmission data rate) and propagation time for transmission across the trunk.

Total time required to deliver the message is a linear sum of all these components of time as they occur in a sequential manner. Delivery time varies from message to message because of random waiting times in queues and alternate routes between the same pair of entry and exist nodes. Therefore, time relationships of the messages and their sequence are the not guaranteed in a store-and-forward sub-network. As traffic increases there is increase in message delivery time because the queues get longer and there may be congestion on the route.

Table 1. Features of Circuit & Store & Forward Switching

Feature	**Circuit Switching**	**Store-&-Forward Switching**
Connection set-up	Connection set-up phase required Finite connections set-up delay	Connection not required to be set-up
Disconnection phase	Required	Not required
Destination address	Specified once	Specified on each message
Delivery delay	Constant delivery delay	Delivery delay is significant and random.

Temporal order	Temporal order is maintained	Temporal order is not maintained.
Time relationship	Message-to-message time relationship is maintained.	Time relationship between two messages is not retained.
Error checking	No error checking	Some transit error control is possible.
Uni/Bi-directional	Bi-directional	Unidirectional
Message delivery	Very high probability of delivery	Delivery is not guaranteed.
Busy hour	Increased connection set-up delay.	Increased delivery delay.
Data rate conversion	Usually changing data rate is not feasible.	Data rates at user ends can be different.

1.5.2 Packet Switching

In message switching, a message is transmitted by a node to another node after it has been completely received. This results in significant delivery delay as we saw in the last section. This delay can be reduced by dividing the message into smaller chunks of data called packets. How this happens is illustrated in Fig.8. Now, each packet can be transmitted by a node to the next node immediately after it is received. Note that total delivery time is not linear sum of all components of delay as there is some overlapping. The total delivery time thus gets reduced. There is some increase in the processing time at the entry and exit nodes because the message needs to be partitioned into packets at the entry node and reassembled at the exit node.

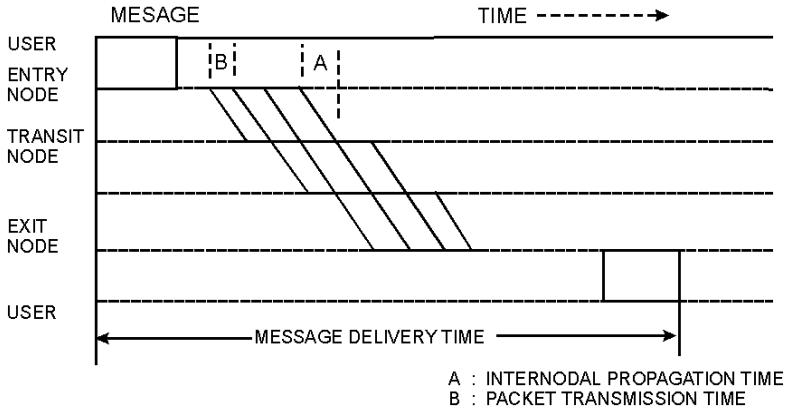


Figure 8: **Time Diagram for packet switching**

Another feature of packet switched networks which results in reduced processing time at the nodes is that the packets are stored in primary memory of the node. Messages on the

other hand are required to be stored in secondary memory because of their size. Access time of primary memory is much less than the secondary memory. In fact delivery time can be so much reduced that users can have even interactive type of dialogue.

The basic packet switching operation of the sub-network is based on store and forward mechanism. The only motivation for packetisation is to reduce the delivery time. As we shall see later, most of the additional features of packet switching have been possible due to reduced delivery time.

1.6 DATAGRAMS AND VIRTUAL CIRCUITS

There are two approaches for routing the data packets through a sub-network:

- Datagram routing
- Virtual circuit routing

In its simplest form, a datagram is a packet of data with the complete address of a destination. Datagrams are sent out onto the sub-network one by one, and the sub-network interprets the destination address on each packet at each stage of switching and tries to deliver it to the destination independent of other datagrams. It is similar to message switching described above except that size of message is limited.

In virtual circuit approach, packets are delivered to the destination over a fixed route which is established beforehand. We shall look at both these approaches in some detail with following sections.

1.6.1 Datagram Routing

Fig. 9 shows a sub-network consisting of five store-and-forward nodes 'A' to 'E' connected by point to point trunk circuits. To send a datagram across the sub-network, it

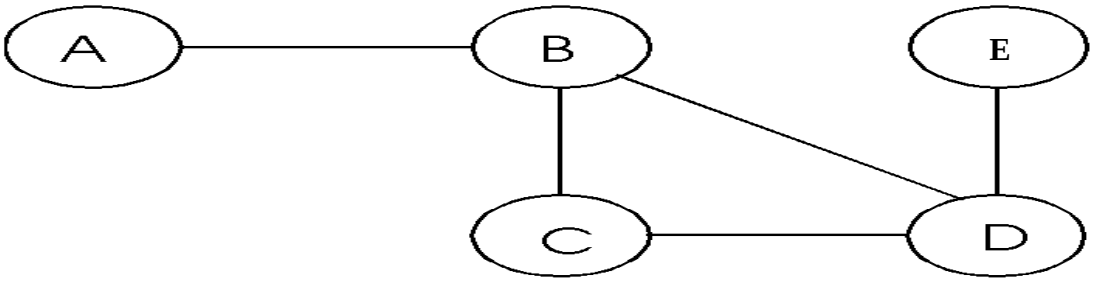


Figure 9: **Datagram routing**

is first sent the user to the access node. In each node, the controlling program examines the designation address on the datagram and uses some algorithm to choose the next link to send the datagram towards its destination.

Some of the possible alternatives for deciding the route of the datagram across the sub-network are:

- Send the datagram to one of the trunk circuits at random. Though the datagram will eventually reach the destination, the method would be very inefficient.
- Another similar approach could be sending it on the trunk which has the shortest queue irrespective of its destination.
- A brute force approach could be to send the datagram on all the trunks. The datagram would reach the destination quickly but large redundant traffic would be generated in the sub-network.
- A much better approach than those mentioned above is to set up a routing table at each node. Given an address, the node can look up the routing table and decide the next link, e.g. to send a datagram from sender 'S' to destination 'R', the routing table at node 'A' would indicate the next link connecting to node 'B'. Similarly at node 'B', the routing table would indicate that the datagram should be sent to node 'D'. The diagram would be next routed to node 'E' and finally to the destination.

The approach seems to be feasible, but we have not considered a very important aspect, updating of routing tables. If a new node is added to the sub-network, all the routing tables at various nodes need to be updated.

1.6.2 Dynamic Routing

Suppose in Fig.9 nodes A, B, C and D are all connected and have up-to-date routing tables, i.e. they have entries for nodes A, B, C and D but there is no entry for node E. Now imagine node E is added to the sub-network as shown in the figure9. The algorithm used for updating the routing tables is that each node will send the updation information to the other nodes it is connected to. When node E becomes active, it will update routing table of node D, node D will in turn, update routing tables of nodes B and C, and node B will update routing table of node A. Another piece of information required for the routing table is number of hops, e.g. distance from node B to node E is two hops via node D and three hops via nodes C and D. so node D will tell B and C one hop distance to E. B and C will note it down as two hops distance to E via D, adding another hop. C will also inform B about E. It will indicate two hops distance to E. Therefore, B will have two alternative routes to E, one of two hops via D and the other of three hops via C. Thus, all the nodes will have updated routing tables.

1.6.3 Congestion And Deadlock

Store-and-forward routing is efficient so long as traffic is sufficiently low. In heavy traffic conditions, datagram movement across the sub-network can stop altogether. To understand this, let us consider a sub-network consisting of three store-and-forward nodes A, B and C (Fig. 10).

Suppose that each node has a finite buffer and each buffer is full with datagrams to be sent to other nodes. In order for node A to be able to send a datagram to node B, node B must have a free buffer to accommodate the datagram. To have a free buffer, node B needs to send a datagram to node C. Since node C is also full and C also cannot send a

datagram to node A to create a free buffer, no movement of datagrams within the sub-network is possible. In other words, there is a deadlock. It is a condition that must never occur. There are two approaches to avoid deadlock. One simple way is to monitor the vacant buffer at each node. Inward flow of the traffic can be stopped when the buffer nears being completely full. But this approach does not eliminate a deadlock situation. Moreover, part of available storage remains unutilized.

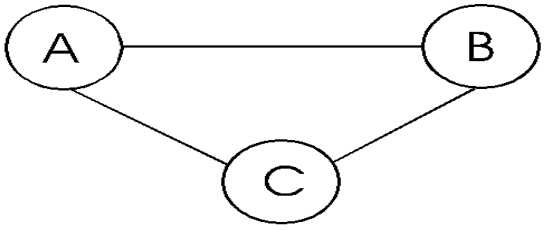


Figure 10: **Store and Forward Nodes**

To avoid an incipient deadlock, another way is to discard some of the datagrams. At first it may not sound a proper way to handle the situation. But a little thought will reveal that it is quite appropriate approach to handle a deadlock situation. Having a deadlock is worse than losing an odd datagram. At least some datagrams will get through and error recovery procedures could be brought into play by the end systems, if there is some movement of datagrams. Those datagrams which have been resident in the buffer for the longest are usually discarded. The end systems have built-in timers and if a data packet is not acknowledged within a specified time, procedure for re-transmission of the packet is initiated. Therefore, the discarded datagrams will be taken care of eventually. In fact, all the datagrams which have spent more than their lifetime in the sub-network should be discarded to avoid duplication of datagrams.

1.6.4 Virtual Circuit Routing

In the virtual circuit approach, a logical connection is established through the sub-network before sending any user data (as done in circuit switched sub-networks). Unlike the datagram approach, the nodes do not make a routing decision for each packet. It is made once for each connection at the time of establishing the connection. Let us understand how it is done. Fig. 11 shows a simple network with user S attached to node A. User S is identified by its address

A-S (usually part of address of a user identifies the node to which it is attached). Another user R with address D-R is attached to node D. Suppose S wishes to exchange data with R. To establish a connection to R, S sends a CONNECT REQUEST packet to node A specifying the destination address D-R. It also specifies a label N_1 to the node.

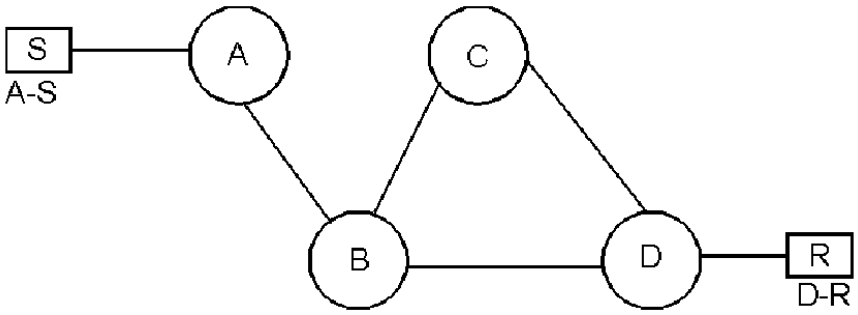


Figure 11: **Network for Virtual Circuit Routing**

Note that S is also requesting the node to use label N1. On receipt of this CONNECT REQUEST, node A takes note of the label N1. Node A examines the destination address specified in the CONNECT REQUEST packet and works out the next link in the chain leading to the destination from its routing table. For this link to node B, node A selects another label N2 which is unique on this link. Node A writes this label by the side of previous label N1. All the future packets of the connection being established and going between node 'A' and node 'B' shall bear label N2. For now, node 'A' sends a modified CONNECT REQUEST packet to node 'B' :

"Connect A-S to D-R. use label N2 for this link".

Note that the label has been changed. On receipt of this packet, node B works out the route and forwards the packet to node 'D' using another label N3. Node 'B' also keeps a record relating labels N2 and N3. Node 'D' sends an INDICATION of incoming call to destination 'R'. It does so using still another label N4 which is unique on the link between node 'D' and 'R'. If 'R' is ready to accept the call, it sends its ACCEPTANCE to node 'D'. It uses label N_4 already being in use for this link of the connection. Node 'D' sends this ACCEPTANCE to node 'B' using label N_3. Node 'B' towards this to node 'A' using label N_2. Node 'A' finally sends a CONFIRMATION to 'S' of having established a connection to the destination. This confirmation bears label N_1.

Thus, in the connection establishment phase, a route to the destination is finalized and a confirmation is received from the destination. The connection is in the form of tables relating the labels of data packets. These tables are maintained at each node (Fig. 12). Whenever a packet is received by a node, it looks up in therein. It also gives to the packet a new label which is also indicated in the table. This connection is called virtual because it does not physically exist.

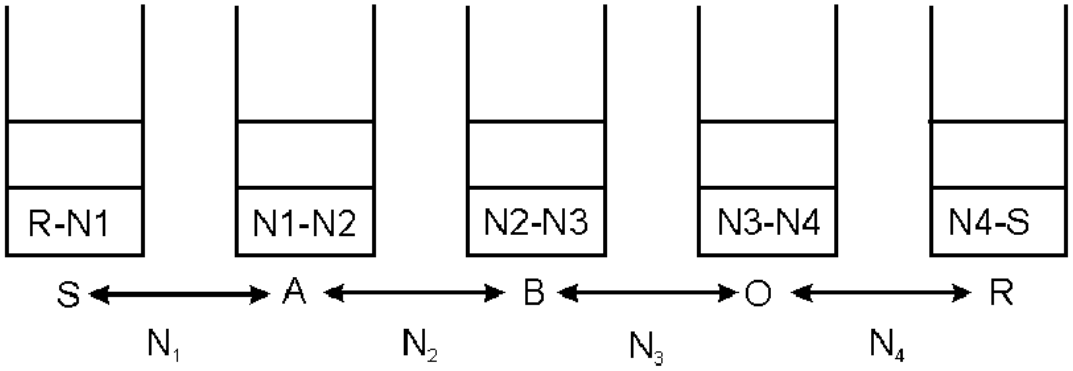


Figure 12: **Tables Maintained at Nodes**

'S' can send data packets now. It will use label N_1 and 'R' will use label N_4 on their packets. Addresses of the destinations are not needed in the data packets

1.7 CONCLUSION

A switched data sub-network consists of an interconnected collection of nodes. The node interconnecting links are called trunks. Data is transmitted from source to destination by being routed through these nodes. At each node, there is need to decide the route through trunk circuits which finally lead to the exit node. This switching function and other related functions are carried out at the nodes. In packet switching sub-networks, the message is first divided into smaller packets of data and then these packets are switched through the sub-network.

2 ROUTING PRINCIPLE

2.1 LEARNING OBJECTIVES

- Router Functions
- Router Operations
- Router Components
- Important Commands
- Routing Principles
- Routing Types & Router Configuration

2.2 INTRODUCTION

In today's era of communication with the evolution of the internet, the main expectation from communication devices is to provide global connectivity with a local presence. The networking devices such as routers play a very vital role in provision of such services. One can work in SOHO environment without routers but for medium and large sized organizations/Units the routers presence is inevitable. The primary function of a packet switching network is to receive packets from a source and deliver them to the destination. To achieve this, a path or route through the network has to be determined. This requires a routing function/ algorithm to be implemented.

2.3 WHAT IS ROUTER?

A router is a device that forwards packets between networks. This forwarding is based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network.

Routing table information can be gathered automatically by routers using some standard type of routing protocols viz distance vector, link state or path vector protocols. Operators can also enter network information in the routing table manually. Using this information, the router chooses the path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support

Traditionally routers were implemented in Software. Software implementation provided High degree of flexibility but the performance was limited because of the slow speed of the processor.

2.4 FUNCTIONS OF ROUTER

- Interconnect communication links.
- Linking WANs and LANs
- Router routes packets as they travel from one network to another network.

- Path determination and packet switching
- Application of security rules (ACLs)
- Protocol conversion (encapsulation)
    - E.g. HDLC, PPP etc.

2.5 ROUTER OPERATION

- Accepts PDUs from incoming network.
- Examines PDU Header.
- Identify the paths available towards the destination with the help of routing table.
- Decide the best path based on different matrics.
- Passes PDU on to next node towards the destination.

2.6 PATH DETERMINATION

- Router accepts packet and views inside Network Layer header
- IP address of destination carried in Network Layer header and other information.
- Destination IP address looked up in routing table
- Packet passed to appropriate exit interface

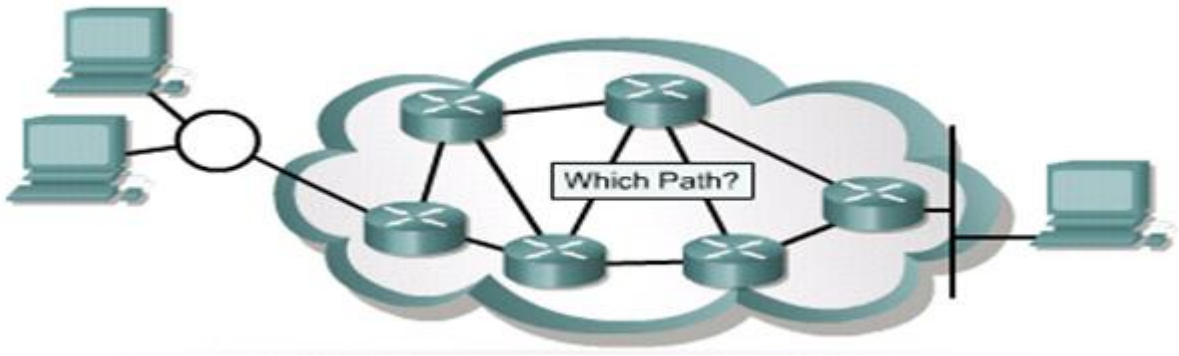


Figure 13: **Layer 3 functions to find the best path through the internetwork**

2.7 TRANSPORT LAYER DETERMINATION

- Transport Layer header contents examined
- Source and destination port checked
- May trigger security of an Access Control List

- May drop packets under heavy load

2.8 ACCESS CONTROL LIST

- Used to identify incoming packets
- Can be used for security purposes
- E.g. do not allow TELNET traffic
  - Identified by destination port number 23
  - Found in Transport Layer header

2.9 ROUTER COMPONENTS

A router is a special type of computer. It has the same basic components as a standard desktop PC. It has a CPU, memory, a system bus, and various input/output interfaces.

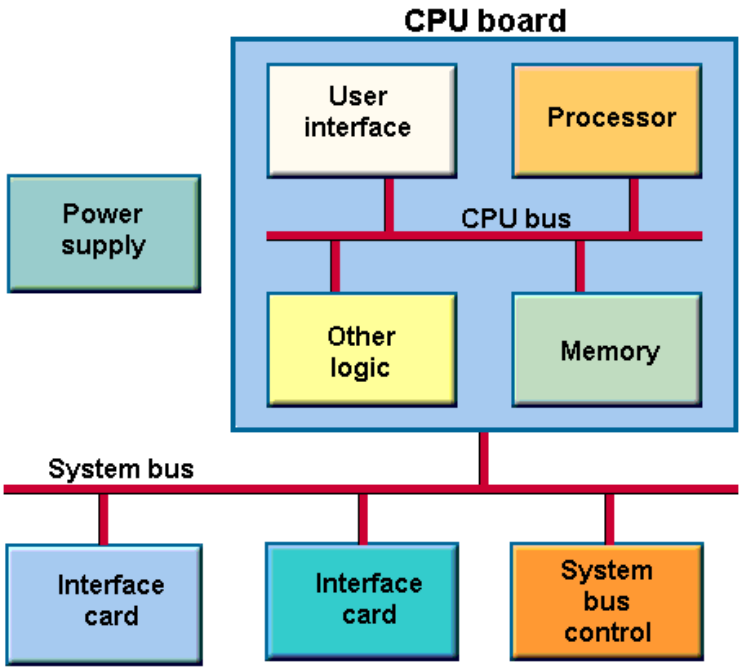


Figure 14: **Basic components of a router**

2.10 MEMORY ELEMENTS OF A ROUTER

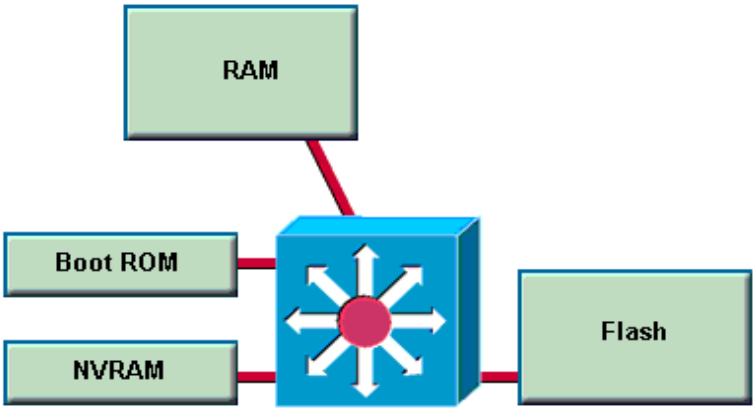


Figure 15: **Memory elements of a router**

2.10.1 Boot Rom

It stores the mini IOS (Internetwork Operating System) image (RX Boot) with extremely limited capabilities and POST routines and core level OS for maintenance.

- Maintains instructions for power-on self test (POST) diagnostics
- Starts and maintains the router
- Stores bootstrap program and basic operating system software
- Requires replacing pluggable chips on the motherboard for software upgrades

2.10.2 Flash

It is an EPROM chip that holds most of the IOS Image. It maintains everything when router is turned off.

- Holds the IOS image
- Allows software to be updated without removing and replacing chips on the processor
- Retains content when a router is powered down or restarted
- Can store multiple versions of IOS software
- Is a type of electrically erasable programmable read-only memory (EEPROM)

2.10.3 RAM

RAM holds running IOS configurations and provides caching. RAM is a volatile memory and loses its information when router is turned off. The configuration present in RAM is called Running configuration.

- Provides temporary memory for the configuration file of a router while the router is powered on.
- Stores routing tables
- Maintains packet-hold queues
- Loses content when a router is powered down or restarted

2.10.4 NVRAM

It is a rewritable memory area that holds the router's configuration file. NVRAM retains the information when ever router is rebooted. Once configuration is saved, it will be saved in NVRAM and this configuration is called Startup Configuration.

- Provides storage for the startup configuration file
- Retains content when a router is powered down or restarted

2.11 EXTERNAL COMPONENTS OF A ROUTER

2.11.1 Interfaces

- Connect routers to a network for packet entry and exit
- Can be on the motherboard or on a separate module

2.11.2 Type Of Interfaces

- The three basic types of connections on a router are
  - LAN interfaces,
  - WAN interfaces,
  - Management ports.

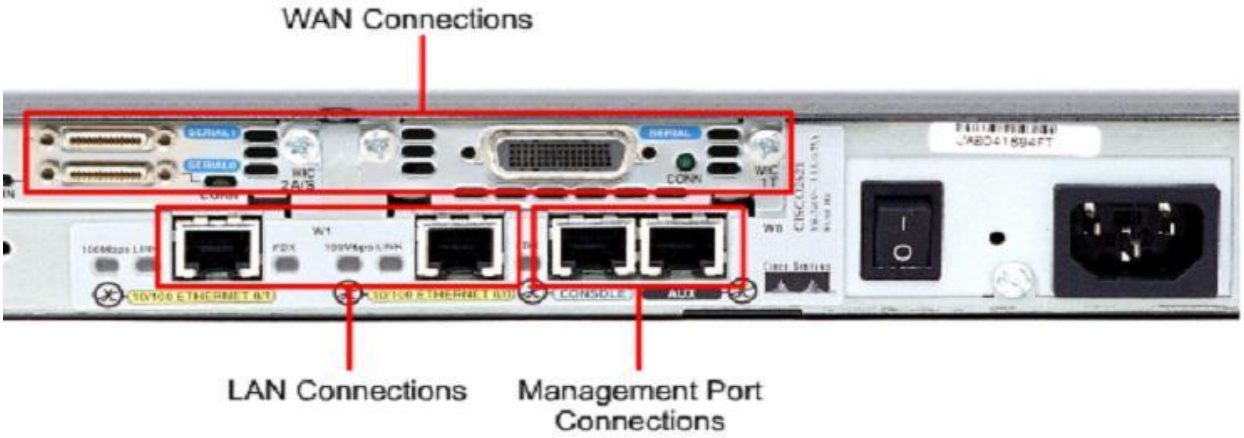


Figure 16: **Interfaces**

- LAN interfaces allow the router to connect to the Local Area Network media.
- Wide Area Network connections provide connections through a service provider to a distant site or to the Internet.
- The management port provides a text-based connection for the configuration and troubleshooting of the router.
- The common management interfaces are the console and auxiliary ports.

2.12 ROUTE SWITCH PROCESSORS

A generic router model requires at least one Route Switch Processor (RSP), which can be procured in three ways: as part of an initial system, as a spare, or as an upgrade.

The RSP is the base system processor module for a router. The RSP contains the system CPU and system memory components. It maintains and executes the management functions that control the system.

Router's images reside in Flash memory, or on as many as two Flash memory cards. Storing IOS images in Flash memory allows you to download and boot from upgraded images remotely. This eliminates the need to remove and replace ROM devices for software updates.

2.13 POWER SUPPLIES

Most of the medium size and high end routers support dual power supplies. The optional additional power supply system provides dual load-sharing for protection against system interruption if one power supply system or one source of power fails.

Note Both dual power supplies must be AC-input or DC-input. The routers do not support mixed power supply types.

2.14 IMPORTANT SHOW COMMANDS

#show access-lists	List access lists
#show arp	Arp table
#show cdp	CDP information
#show clock	Display the system clock
#show controllers	Interface controllers status
#show crypto	Encryption module
#show debugging	State of each debugging option
#show dhcp	Dynamic Host Configuration Protocol status
#show flash:	display information about flash: file system
#show frame-relay	Frame-Relay information
#show history	Display the session command history
#show hosts	IP domain-name, lookup style, name servers, and host table
#show interfaces	Interface status and configuration
#show ip	IP information
#show ospf	For OSPF debug only
#show ospfv3	For OSPFv3 debug only
#show processes	Active process statistics
#show protocols	Active network routing protocols
#show running-config	Current operating configuration
#show sessions	Information about Telnet connections
#show ssh	Status of SSH server connections
#show startup-config	Contents of startup configuration

#show tcp	Status of TCP connections
#show terminal	Display terminal configuration parameters
#show users	Display information about terminal lines
#show version	System hardware and software status

2.15 ROUTER BASIC CONFIGURATION

2.15.1 Management Port Connections

When the router is first put into service, there are no networking parameters configured. To prepare for initial startup and configuration, attach an RS-232 ASCII terminal, or a computer emulating an ASCII terminal, to the system console port. Then configuration commands can be entered to set up the router.

2.15.2 Console Port Connection

a. The console port is a management port used to provide access to the router. It is used for the initial configuration of the router, monitoring, and disaster recovery procedures.
b. To connect to the console port, a rollover cable and a RJ-45 to DB-9 adapter are used to connect a PC. Cisco supplies the necessary adapter to connect to the console port.
c. The PC or terminal must support VT100 terminal emulation.
d. Terminal emulation software such as HyperTerminal is usually used.

2.16 AUXILIARY PORT CONNECTION

a. The router can also be configured from a **remote location** by dialing to a modem connected to the auxiliary port on the router.

2.17 ROUTER OPERATING SYSTEM

- A router or switch cannot function without an OS
- Router Operating system is known as Internetwork Operating System (IOS)
- Operating system stores in Flash memory (non-volatile)

2.18 OPERATION OF IOS SOFTWARE

The startup process of the router normally loads into RAM and executes one of 3 operating environments:

- ROM monitor: Performs the bootstrap process and provides low-level functionality and diagnostics. Used to recover from system failures and recover from a lost password. Available only through console.
- Boot ROM: limited subset of the Cisco IOS. Allows write operations to flash memory and is used primarily to replace the Cisco IOS image that is stored in flash ex: copy tftp flash
- Cisco IOS : Stored in Flash, but loaded and executed from RAM

2.19 INITIAL STARTUP OF CISCO ROUTERS

The startup routines done to start the router operations must accomplish the following:

- Make sure that the router hardware is tested and functional i.e. the CPU, memory, and interfaces
- Find and load the Cisco IOS software.

Find and apply the startup configuration file or enter the setup mode.

After the POST, the following occur as the router initializes:

- The generic bootstrap loader in ROM executes
  - The bootstrap loads instructions that cause other instructions to be loaded
- The operating system is loaded
  - The location is disclosed in the boot field of the configuration register
- The operating system locates the hardware and software components and lists the results on the console terminal
- The configuration file saved in NVRAM is loaded into main memory and executed one line at a time
  - The commands start routing processes, supply addresses for interfaces, and define other operating characteristics of the router
- If no configuration file is found, the operating system enters setup mode

2.20 ROUTER USER INTERFACE MODES

The IOS provides a command interpreter service known as the command executive (EXEC). The EXEC validates and executes the command

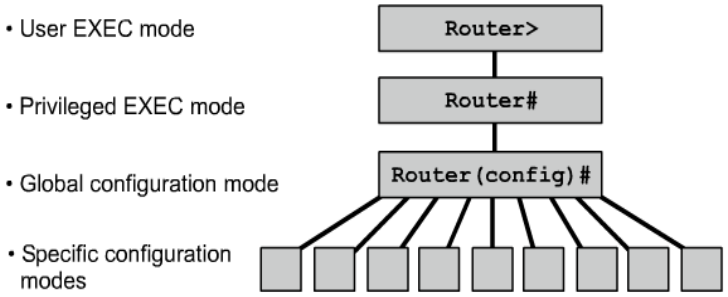
The EXEC session is separated in two 2 levels of access

User EXEC mode – allows the user to check the router status. No router configuration changes are allowed.

- > router

Privileged EXEC mode (Enable Mode) – allows the user to change the router configuration

- router#
- Enter the **enable** command at the ">" prompt
- Enter configuration and management commands



Configuration Mode	Prompt
Interface	`Router(config-if)#`
Subinterface	`Router(config-subif)#`
Controller	`Router(config-controller)#`
Map-list	`Router(config-map-list)#`
Map-class	`Router(config-map-class)#`
Line	`Router(config-line)#`
Router	`Router(config-router)#`
IPX-router	`Router(config-ipx-router)#`
Route-map	`Router(config-route-map)#`

Figure 17: **Router user interface modes**

2.21 ROUTER CONFIGURATION

2.21.1 Configuring A Router Name

Router#config t

Router(config)#hostname BSNL

BSNL(config)#

2.22 BACKUP AND RESTORE

2.22.1 Copy Running-Configuration File

Router#copy running-config tftp

Address or name of remote host [ ]? 10.10.10.2

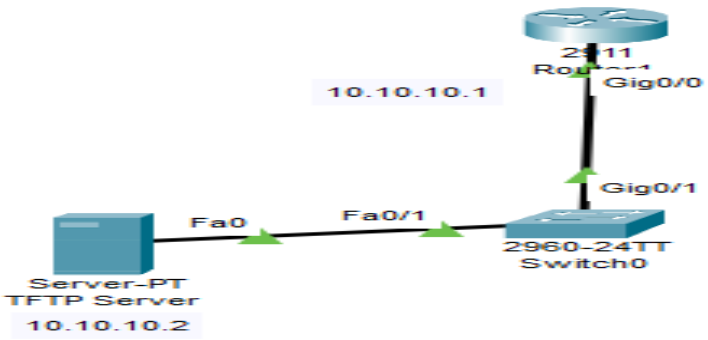


Figure 18: **Destination filename**

Writing running-config...!!

[OK - 497 bytes]

Router#copy tftp running-config

Address or name of remote host [ ]? 10.10.10.2

Source filename [ ]? RC

Destination filename [running-config]?

Accessing tftp://10.10.10.2/RC...

Loading RC from 10.10.10.2: !

[OK - 497 bytes

2.22.2 Backup And Restore IOS

Router#show flash

System flash directory:

File Length Name/status

3 33591768 c2900-universalk9-mz.SPA.151-4.M4.bin

2 28282 sigdef-category.xml

1 227537 sigdef-default.xml

Router#copy flash tftp

Source filename []? c2900-universalk9-mz.SPA.151-4.M4.bin

Address or name of remote host []? 10.10.10.2

Destination filename [c2900-universalk9-mz.SPA.151-4.M4.bin]? 2911IOS

Router#copy tftp flash

Address or name of remote host []? 10.10.10.2

Source filename [ ]? 2911IOS

Destination filename [2911IOS]? c2800nm-advipservicesk9-mz.124-15.T1.bin

%Warning:There is a file already existing with this name

Do you want to over write? [confirm]y

Erase flash: before copying? [confirm]y

Erasing the flash filesystem will remove all files! Continue? [confirm]y

Erase of flash: complete

Accessing tftp://10.10.10.2/2911IOS...

Loading 2911IOS from 10.10.10.2

2.23 ROUTING PRINCIPLES

The basic attributes of routing are as follows:-

- Correctness
- Simplicity
- Robustness
- Stability
- Fairness
- Optimality
- Efficiency

Robustness has to do with the routing of packets through alternate routes in the network in case of route failures or overloads

Stability is an important aspect of the routing algorithm. It implies that the routing algorithm must converge to equilibrium as quickly as possible, however some never converge, no matter how long they run.

Fairness and optimality are competing requirements. A trade-off exists between the two. Some performance criteria may give a higher priority to transportation of packets between

adjacent/ nearby stations in comparison to those between distant stations. This results in higher throughput but is not fair to the stations which have to communicate with distant stations.

Efficiency of a routing technique/ algorithm gets decided by the quantum of overhead processing required. Of course these have to be kept to a minimum.

Thus, Routing is essentially a method of path selection and is an overhead activity.

2.24 ROUTING & NETWORK LAYER ADDRESSES

Routers relay a packet from one data link to another. To relay a packet, a router employs two basic functions:

- a path determination function and
- a switching function.

Figure illustrates how routers use the addressing for routing and switching functions. When a packet destined for network 100.1.0.0 arrives at Router 1, the router knows that the packet should be sent out on port S0.

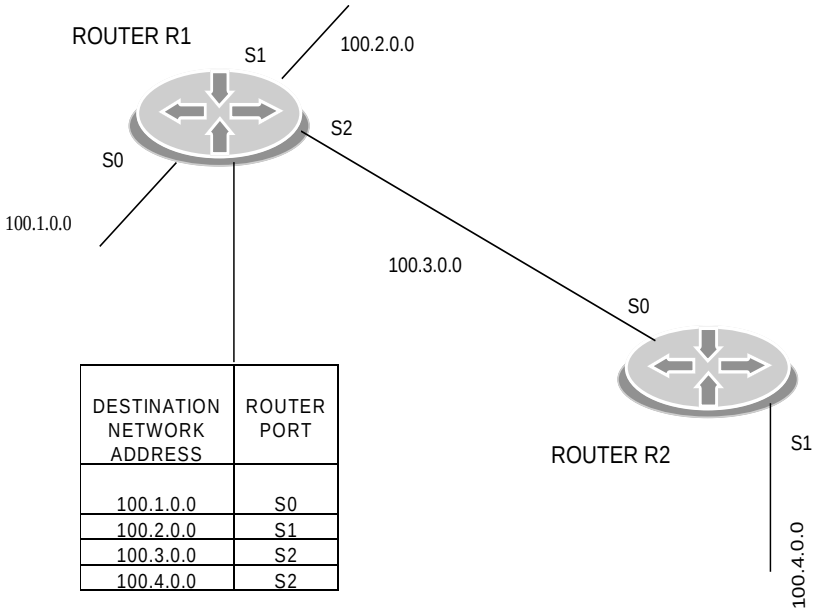


Figure 19: **Routing table example**

2.25 USE OF NETWORK LAYER ADDRESS IN ROUTING

From the router to the destination, a router is responsible only for passing the packet to the best network along the path. This best path is represented as a direction to a destination network. For example, in figure 2, if a packet that is destined for network 100.4.0.0 arrives at Router 1, the router knows that the best direction to send the packet out is interface S2. Router 2 is the next hop, or router, along the path. The router uses the network portion of the address to make these path selections.

The switching function enables a router to accept a packet on one interface and forward it on a second interface. The path determination function enables the router to select the most appropriate interface for forwarding a packet.

Routing assumes that addresses have been assigned to network elements to facilitate data delivery. In particular, routing assumes that addresses convey at least partial information about where a host is located. This permits routers to forward packets without having to rely either on broadcasting or a complete listing of all possible destinations. At the IP level, routing is used almost exclusively, primarily because the Internet was designed to construct large networks in which heavy broadcasting or huge routing tables are not feasible.

2.26 THREE GENERAL PREREQUISITES MUST BE MET TO PERFORM ROUTING

DESIGN A plan must exist by which addresses are assigned. Typically, addresses are broken into fields corresponding to levels in a physical hierarchy. At each level of the hierarchy, only the corresponding field in the address is used, permitting addresses to be handled in blocks. In ip, the most common designs are ip address classes, sub-netting, and cidr.

IMPLEMENTATION : the design plan must be implemented in switching nodes, which must be able to extract path information from the addresses. since router programming is generally not under a designer's control, designs must be limited by the features provided by manufacturers. subnetting's great appeal lies in its great flexibility, while using a fairly simple implementation model.

ENFORCEMENT : the plan must be enforced in host addressing. A design is useless unless addresses are assigned in accordance with it. Addressing authority must be centralised.

In the Internet environment, routing is almost always used at the IP level, and bridging almost always used at the Data Link Layer.

For new network installations, the best approach is to plan for routing even if it's not used at first. This requires some advanced planning to design an addressing scheme that will work. However, the overhead is all human - hardware won't know the difference between organised and haphazard addressing schemes. Network should be planned for the ability to put routers in strategic locations, even if those locations will initially use bridges or just signal boosters (such as Ethernet hubs and repeaters). In this manner, routers can be easily added later.

2.27 ROUTED PROTOCOL

A routed protocol is a protocol that contains sufficient network-layer addressing information for user traffic to be directed from one network to another network. Routed protocols define the format and use of the fields within a packet. Packets that use a routed protocol are conveyed from one end system to another end system through an internetwork.

The internet protocol IP and Novell's IPX are examples of routed protocols.

2.28 ROUTING PROTOCOL

A routing protocol provides mechanisms for sharing routing information. Routing protocol messages move between the routers. A routing protocol allows the routers to communicate with other routers to update and maintain routing tables. Routing protocol messages do not carry end-user traffic from network to network. A routing protocol uses the routed protocol to pass information between routers.

2.29 TYPES OF ROUTING: STATIC, DEFAULT, DYNAMIC

2.29.1 Static Routing:

Refers to routes to destinations being setup manually in the router. Network reachability in this case is not dependent on the existence and state of the network itself. Whether a destination is up or down, the static routes would remain in the routing table, and traffic would still be sent towards that destination. Static routing generally is not sufficient for large or complex networks because of the time required to define and maintain static routte table entries.

2.29.2 Default Routing:

Refers to a "last resort" outlet – traffic to destinations that are unknown to the local router are sent to the default outlet router. Default routing is the easiest form of routing for a domain connected to a single exit point. A default route is a path on which a router should forward a packet if it does not have specific knowledge about the packet's destination. Figure below illustrates the concept of Static and default Routing.

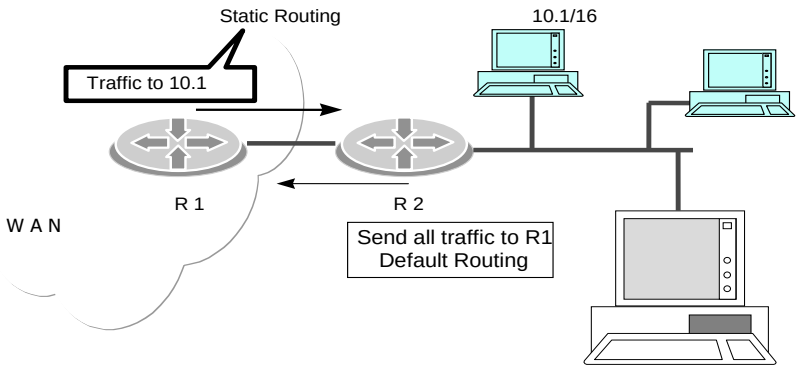


Figure 20: **Static and Default Routing**

2.29.3 Dynamic Routing

Refers to routes being learnt via an internal or external routing protocol. Network reachability is dependent on the existence and state of the network. If a destination is down, the route would disappear from the routing table, and traffic will not be sent toward the destination. Dynamic routing is used to enable routers to build their routing tables automatically and make the appropriate forwarding decisions. This concept is illustrated in Figure below.

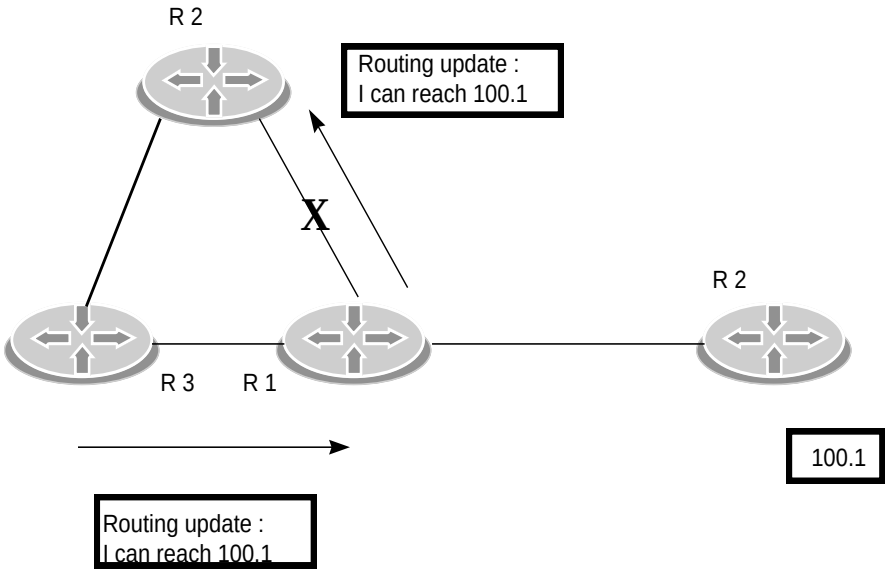


Figure 21: **Dynamic Routing**

Static and default routing is not our enemy. The most stable (but not so flexible) configurations are the ones based on static routing. Many people feel that they are not technologically up-to-date because they are not running dynamic routing. Trying to force dynamic routing on situations that do not really need it is just a waste of bandwidth, effort, and money.

As networks keep on growing in size, the routing tables also grow proportionately. Considerable amount of router memory is consumed by these ever increasing tables. In

addition, the processor time is eaten up in scanning these tables and bandwidth is consumed in sending status reports about the updated routing tables. At a certain stage, the network size becomes so large that it becomes impossible to have every router keep an entry of every other router in the network. Ultimately, the routing has to be done **hierarchically**, similar to a telephone network.

2.30 ROUTING ALGORITHMS

Routing algorithms and protocols form the core of the hacker's Internet, because it is here that all the decisions get made. Network engineers assign costs to network paths, and routing protocols select the least-cost path to the destination.

Routing protocols bear a resemblance to capitalist market economics. In both systems, there is a large group of "nodes", the decisions of each being driven by a cost-minimisation algorithm. The end result is a reasonably efficient distribution of "resources". Furthermore, cost determination is done in similar ways. A router, like an import/export firm, will compute its cost, add on profit for its part in the transaction, and pass this cost along to customers. Both systems use this method to achieve reasonable efficiency.

Routing is the main process used by Internet hosts to deliver packets. Internet uses a hop-by-hop routing model, which means that each host or router that handles a packet examines the Destination Address in the IP header, computes the next hop that will bring the packet one step closer to its destination, and delivers the packet to the next hop, where the process is repeated.

To make this work, two things are needed:

First, routing tables match the destination addresses with next hops.

Second, routing protocols determine the contents of these tables.

Routing algorithms can be grouped into two major classes:

- Non-Adaptive or Static
- Adaptive or Dynamic

NON-ADAPTIVE ALGORITHMS do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J (for all I to J) is computed in advance, off-line, and downloaded to the routers when the network is booted. This procedure is also called as **Static Routing**.

ADAPTIVE ALGORITHMS change their routing decisions to take into account changes in the topology, and sometimes the traffic as well. Adaptive algorithms will be

classified depending on where it gets the information from - whether locally, from adjacent Routers, or from all Routers

When does the algorithm decide to change the routes - whether every ΔT sec, when the load changes, or when the topology changes, and what metric (parameter) is used for optimization i.e. either distance, number of hops, or estimated transit time.

2.31 DYNAMIC ROUTING OPERATIONS

The success of dynamic routing depends on two basic router functions:

- Maintenance of a routing table
- Timely distribution of knowledge – in the form of routing updates – to other routers

Dynamic routing relies on a routing protocol to disseminate knowledge. A routing protocol defines the set of rules used by a router when it communicates with neighboring routers. Typically, a routing protocol describes:

- How updates are conveyed
- What knowledge is conveyed
- When to convey this knowledge
- How to locate recipients of the updates

2.32 REPRESENTING DISTANCE WITH METRICS

When a routing algorithm updates the routing table, its primary goal is to determine the best information to include in the table. Each routing algorithm will interpret “best” in its own way. The algorithm generates a number – called the metric- for each path through the network. Typically, the smaller the metric, the better is the path.

Metrics can be calculated based on a single characteristic of the path or by combining several key characteristics such as:

Hop Count -refers to the number of routers a packet must go through, to reach a destination. The lower the hop count, the better is the path. Path length is used to indicate the sum of the hops to a destination.

Cost -path cost is the sum of cost associated with each link to a destination. Costs are assigned (automatically or manually) to the process of crossing a network. Slower networks typically have a higher cost than faster networks. The lowest ‘cost” route is the one believed to be the fastest route available.

Bandwidth -the rating of a link's throughput. Routing through links with greater bandwidth does not always provide the best routes. For example, if a high-speed link is busy, sending a packet through a slower link might be faster.

2.33 INTERIOR ROUTING

Interior routing occurs within an autonomous system. Most common interior routing protocols are **RIP and OSPF**. The basic routable element is the IP network or subnetwork, or CIDR prefix for newer protocols.

2.34 EXTERIOR ROUTING

Exterior routing occurs between autonomous systems, and is of concern to service providers and other large or complex networks. The basic routable element is the Autonomous System, a collection of CIDR prefixes identified by an Autonomous System number. While there may be many different interior routing schemes, a single exterior routing system manages the global Internet, based primarily on the **BGP-4 (Border Gateway Protocol Version 4)** exterior routing protocol.

2.35 INTERFACE CONFIGURATION OF ROUTER 0

Router>en

Router#conf t

Router(config)#int s0/0/0

Router(config-if)#ip address 172.16.16.2 255.255.255.252

Router(config-if)#no shut

Router(config-if)#

Router(config-if)#exit

Router(config)#int fa0/1

Router(config-if)#ip address 10.10.10.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#exit

Router#wr

2.36 INTERFACE CONFIGURATION OF ROUTER 1

Router>en

Router#conf t

Router(config)#int s0/0/0

Router(config-if)#ip address 172.16.16.1 255.255.255.252

Router(config-if)#no shut

Router(config-if)#

Router(config-if)#exit

Router(config)#int fa0/1

Router(config-if)#ip address 20.20.20.1 255.255.255.0

Router(config-if)#no shut

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 152.3.3.1 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#int loopback o

Router(config-if)#ip address 198.168.0.254 255.255.255.255

Router#end

Router#wr

2.37 INTERFACE CONFIGURATION OF ROUTER 2

Router>en

Router#conf t

Router(config)#int fa0/0

Router(config-if)#ip address 152.3.3.2 255.255.255.252

Router(config-if)#no shut

Router(config-if)#

Router(config-if)#exit

Router(config)#int fa0/1

Router(config-if)#ip address 30.30.30.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#exit

Router#wr

2.38 STATIC ROUTING

2.38.1 Route To Be Entered For Router 0

Distance Network ID	Mask	Next HOP	Exit Interface
30.30.30.0	255.255.255.0	172.16.16.1	S0/0/0
152.3.3.0	255.255.255.252	172.16.16.1	S0/0/0
20.20.20.0	255.255.255.0	172.16.16.1	S0/0/0
198.168.0.254	255.255.255.255	172.16.16.1	S0/0/0

Router 0 (config)# ip route 30.30.30.0 255.255.255.0 172.16.16.1/s0/0/0

Router 0 (config)# ip route 152.3.3.0 255.255.255.252 172.16.16.1/s0/0/0

Router 0 (config)# ip route 20.20.20.0 255.255.255.0 172.16.16.1/s0/0/0

Router 0 (config)# ip route 198.168.0.254 255.255.255.255 172.16.16.1/s0/0/0

2.38.2 Route To Be Entered For Router 1

Distance Network ID	Mask	Next HOP	Exit Interface
10.10.10.0	255.255.255.0	172.16.16.2	fa0/0
30.30.30.0	255.255.255.0	152.3.3.2	S0/0/0

Router1 (config)#ip route 10.10.10.0 255.255.255.0 172.16.16.2 /fa0/0

Router1 (config)#ip route 30.30.30.0 255.255.255.0 152.3.3.2 /s0/0/0

2.38.3 Route To Be Entered For Router 2

Distance Network ID	Mask	Next HOP	Exit Interface

20.20.20.0	255.255.255.0	152.3.3.1	fa0/0
198.168.0.254	255.255.255.255	152.3.3.1	fa0/0
172.16.16.0	255.255.255.252	152.3.3.1	fa0/0
10.10.10.0	255.255.255.0	152.3.3.1	fa0/0

Router2(config)#ip route 20.20.20.0 255.255.255.0 152.3.3.1 /fa0/0

Router2(config)#ip route 198.168.0.254 255.255.255.255 152.3.3.1 /fa0/0

Router2(config)#ip route 172.16.16.0 255.255.255.252 152.3.3.1 /fa0/0

Router2(config)#ip route 10.10.10.0 255.255.255.0 152.3.3.1 /fa0/0

2.39 DEFAULT ROUTING

2.39.1 Route To Be Entered For Router 0

Distance Network ID	Mask	Next HOP	Exit Interface
0.0.0.0	0.0.0.0	172.16.16.1	S0/0/0

Router 0 (config)# ip route 0.0.0.0 0.0.0.0 172.16.16.1/s0/0/0

2.39.2 Route To Be Entered For Router 1

Distance Network ID	Mask	Next HOP	Exit Interface
10.10.10.0	255.255.255.0	172.16.16.2	fa0/0
30.30.30.0	255.255.255.0	152.3.3.2	S0/0/0

Router1 (config)#ip route 10.10.10.0 255.255.255.0 172.16.16.2 /fa0/0

Router1 (config)#ip route 30.30.30.0 255.255.255.0 152.3.3.2 /s0/0/0

2.39.3 Route To Be Entered For Router 2

Distance Network ID	Mask	Next HOP	Exit Interface
0.0.0.0	0.0.0.0.	152.3.3.1	fa0/0

Router2(config)#ip route 0.0.0.0 0.0.0.0. 152.3.3.1 /fa0/0

2.40 DYNAMIC ROUTING

2.40.1 Route To Be Entered For Router 0

Directly connected Network ID	172.16.16.0	10.10.10.0

Router0(config)#router rip

Router0 (config-router)#version 2

Router0 (config-router)#network 10.10.10.0

Router0 (config-router)#network 172.16.16.0

2.40.2 Route To Be Entered For Router 1

Directly connected Network ID	20.20.20.0	152.3.3.0	172.16.16.0	198.168.0.254

Router1(config)#router rip

Router1(config-router)#version 2

Router1(config-router)#network 20.20.20.0

Router1(config-router)#network 152.3.3.0

Router1(config-router)#network 172.16.16.0

Router1(config-router)#network 198.168.0.254

2.40.3 Route to be entered for Router 2

Directly connected Network ID	30.30.30.0	152.3.3.0

Router2(config)#router rip

Router2(config-router)#version 2

Router2(config-router)#network 30.30.30.0

Router2(config-router)#network 152.3.3.0

2.41 CONCLUSION

Knowing where and how to send data packets is the most important job of a router. Simple router does this and nothing more. Other routers add additional functions including security features. The one constant is that the modern networks including the internet could not exist without routers. Exterior routing occurs between autonomous systems, and is of concern to service providers and other large or complex networks. While there may be many different interior routing schemes, a single exterior routing system manages the global Internet, based primarily on the BGP-4 (Border Gateway Protocol Version 4) exterior routing protocol.

3 BROADBAND & MULTIPLAY

3.1 LEARNING OBJECTIVES

- Broadband, Definition & Advantages
- Wired Broadband Technologies
- Broadband Multiplay – Components & Architecture
- Broadband Multiplay Services

3.2 WHAT IS BROADBAND?

TRAI has defined Broadband as an always on data connection that is able to support interactive services including internet access and has the capability of minimum download speed of 512 kbps to an individual subscriber from the point of presence (POP) of the service provider intending to provide broadband service where multiple such individual broadband connection are aggregated and the subscriber is able to access these interactive services including the internet through this POP. The interactive services will exclude any service for which a separate license is specifically required, for example, real time voice transmission, except to the extent that it is presently permitted under ISP license with Internet telephony.

3.3 ADVANTAGES OF BROADBAND

- Always on (Not on shared media)
- Fast (> 512 kbps)
- No disconnection
- No additional access charge
- Telephone and Data simultaneously

3.4 WIRED BROADBAND TECHNOLOGIES

There are many different types of broadband access technologies. Each of these technologies can compete to provide similar services to consumers and businesses.

- Digital Subscriber Line (DSL, given over copper loop of Telecom operators)
- Cable Modem (CM, Given over cable TV operators coaxial cable network)
- Power Line Broadband (BPL, Over Power lines)
- Fiber technology

3.5 DIGITAL SUBSCRIBER LINE (DSL)

Digital Subscriber line (DSL) is a wire line transmission technology that brings data and information faster over copper telephone lines already installed in homes and

business. Traditional phone service connects your home or business to a telephone company office via copper wires. A DSL modem accesses the local telephone company's central office where a DSL Access DSLAM then transmits the signal from the copper telephone line onto a network backbone, and eventually to the Internet. With high speed Internet access that uses DSL transmission technology, there is no need to "dial in" to a traditional modem. This service allows consumers and business to have an "always-on" dedicated connection to the Internet. The following are types of DSL transmission technologies that may be used to provide high-speed Internet access.

3.5.1 Symmetrical Digital Subscriber Line (SDSL)

It is used typically for business applications such as video conferencing. The traffic from the user to the network is upstream traffic, and from the network to the user is downstream traffic. When the data rate in both directions is equal, it is called a symmetric service.

3.5.2 Asymmetrical Digital Subscriber Line (ADSL)

It is used primarily by residential users who receive a lot of data but do not send much such as Internet surfers. ADSL provides faster speed in a downstream direction (from the telephone central office to the customer's premises) than upstream (from customer's premise to the telephone central office). When the upstream data rate is lower than the downstream rate, it is called an asymmetric service.

ADSL STANDARDS

Family	Up stream Rate	Down stream	Maximum range
ADSL	640 kbps	8 Mbps	5.5 Km
ADSL2	1-1.5 Mbps	12-16 Mbps	5.7 Km
ADSL2 +	1 Mbps	26 Mbps	5.7 Km

3.5.3 High-Data-Rate Digital Subscriber Line (HDSL)

It provides fixed symmetrical high-speed access at T1 rate (1.5 mbps), and is designed for business purposes.

3.5.4 Very High-Data-Rate Digital Subscriber Line (VDSL)

It provides both symmetrical and asymmetrical access with very high bit rate over the copper line. Deployment is very limited at this time.

3.6 BSNL'S BROADBAND ACCESS TECHNOLOGY

BSNL Broadband service is built on a world class, multi-gigabit, multi-protocol, convergent IP infrastructure through National Internet Backbone-II (NIB-II) that provides convergent services through the same backbone and broadband access network. In BSNL Asymmetric Digital Subscriber Line (ADSL) Technology is used for giving the Broadband connection where greater download is required in comparison to upload.

3.6.1 For Bsnl Broadband Connection, Customer Needs:

- BSNL's Landline connection
- Computer with 10/100 Mbps Ethernet Card
- DSL Modem + Splitter (CPE)
- PPPoE software to be loaded in the Client
- Broadband Account (Username and Password)

3.6.2 Services Offered To Broadband Customers

- Basic Internet Access Service controlled and uncontrolled (512Kbps to 1000Mbps). BSNL has various tariff plans for home and business customers.
- Content Based services: [Video on Demand (VoD), Education, Audio on Demand (AoD) etc.
- Web conferencing: BSNL has tied up with a franchisee to offer this service. Toll free number for knowing details is 1800-111-233. BSNL Web Conferencing Service enables to conduct virtual meetings with business partners, suppliers, employers etc. It has the innovative feature such as Persistent meeting rooms, which simulates physical room environment wherein authorized users can enter their designated rooms the way they do in physical meetings.
- The users can access the rich features, apart from multi-point, multimedia (Audio, Video & Data) conferencing service, BSNL web Conferencing service provides very powerful data conferencing tools to enhance collaboration among users such as sharing of PowerPoint Presentation, Whiteboard, Documents, & Chat facility amongst the conference participants, which will significantly aid in increasing the effectiveness of your business meetings. BSNL Web Conferencing Service does not require expensive end points; all that you require are a PC, Web-cam and an ADSL Connection.
- It is ideally suited for users at all levels in large corporate houses, Small and medium businesses, SOHOs & quality conscious individuals to enhance collaboration, increase productivity and save costs.
- VPN on broadband.
- Bandwidth on Demand (User and or service configurable)

3.7 WHAT IS BB MULTIPLAY?

The triple play service means providing the following service to the customer: -

- Data (Internet)
- Voice (VoIP and not the PSTN which is already provided on broadbandalso)
- Video (IPTV, VoD or in general live broadcast and stored broadcastingusing video streaming protocols)

3.8 COMPONENTS OF BROADBAND MULTIPLAY

The BSNL's Broadband multiplay network consists of the following components:

- L3PE (MCR / PE Router of NIB-2 Project 1 – Supplied by HCL).
- BNG – Broadband Network Gateway (Connects Multiplay Network to NIB2Backbone Project 1, through L3PE).
- RPR (Tier-1 Switch and Tier-2 switches in the ring Provides connectivityto BNG & vice versa).
- OC LAN Tier-2 Switch.
- DSLAM.
- ADSL CPE.
- DSL Tester.

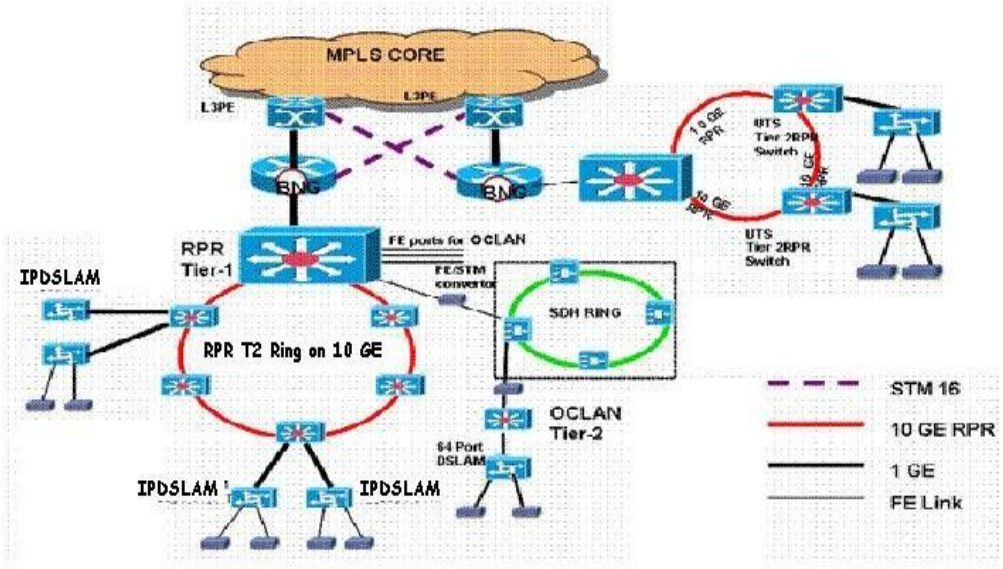


Figure 22: **N/W Architecture Broadband Multiplay**

3.8.1 DSLAM

DSL Access Multiplexor or De-multiplexor.

- Supports PPP and ATM for xDSL services.
- Supports GE and FE connectivity for uplink, cascading, and other types of data connectivity.
- Supports VLAN.

3.8.2 RPR

Resilient Packet Ring (RPR) Switch:

- The traffic from access devices and remote aggregation devices is aggregated in RPR and forwarded to the Core Network.
- Resilience: Proactive span protection automatically avoids failed span within 50ms.
- Ring Topology gives the scalable option of having more than 100 nodes in a ring.
- RPR has the ability to differentiate between low & high priority packets.

3.8.3 Broadband Network Gateway(BNG)

- It routes traffic to and from broadband remote access devices DSLAMs /OLTs on an Internet service provider's (ISP) network.
- It works as Multi Service Edge Router(MSER).
- Service specific logical mini routers are configured in BNG called context or routing instances.
- BNG maps the traffic coming from access networks elements and forward to uplink L3PE VLANs IP MPLS Network through corresponding service context.
- Authentication, Authorization and accounting processes happen via radius servers configured logically in BNG.

3.8.4 Changes In Broadband Multiplay After Broadband

- T1 & T2 changed from star topology to RPR ring topology – High reliability
- IP-DSLAM connected on GE interface as compared to FE interface.
- BNG behaves as a customer edge router whereas BRAS was a PE Router.
- BRAS were present at 23 “A” locations only whereas BNG is present upto “B”type cities.

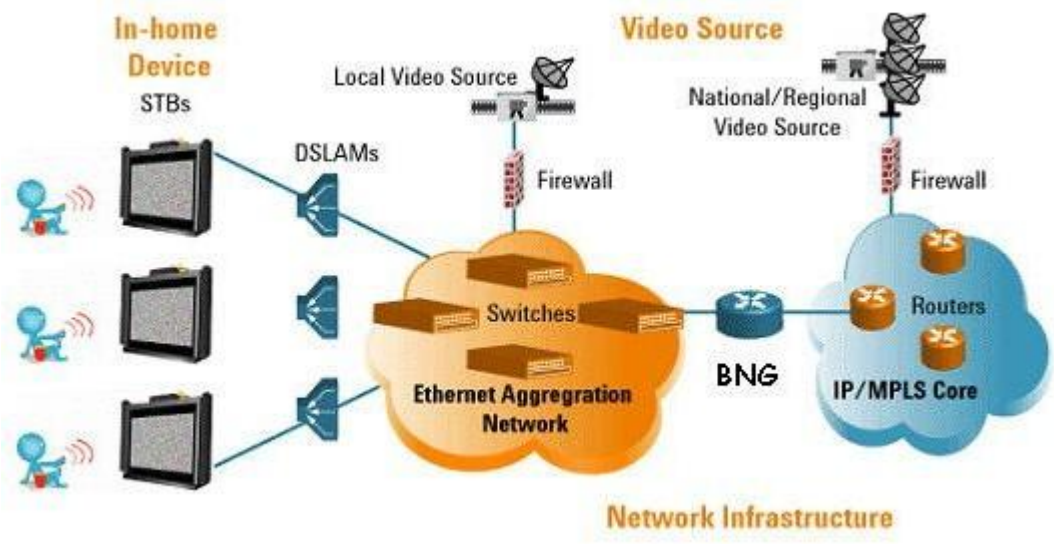


Figure 23: **Network Architecture**

3.9 SERVICES

- IPTV/ TVoIP
- Video on Demand (VoD)
- Games on Demand (GoD)

IPTV or TVoIP delivers television programming to households via broadband connection using Internet protocols. It requires a subscription and IPTV set-top box(STB), this box will connect to the home DSL line and is responsible for reassembling the packets into a video stream and then decoding the contents. IPTV is typically bundled with other services like Video on Demand (VOD), Voice Over IP (VOIP) or digital Phone, and Web access. IPTV viewers will have full control over functionality such as rewind, fast-forward, pause, and so on.

If you've ever watched a video clip on your computer, you've used an IPTV system in its broadest sense. The video stream is broken up into IP packets and dumped into the core network, which is a massive IP network that handles all sorts of other traffic (data, voice, etc.). VOD (Video on Demand) service allows the user the luxury of watchingthe movie of his / her choice at his / her convenience.

3.10 DIFFERENCE BETWEEN VOD ON BB & VOD ON DTH

In DTH, as it is broadcasting and not communication so the request for VOD has to be registered through some other mean than the Set top Box say can be through

phone call, SMS or Internet and the same four to five movies are broadcasted and the viewers have to choose among them only and at predefined timings.

In true VOD, as offered by BSNL, the set-top box behaves just like a DVD player and viewer can select a movie from the boutique, view it at his / her desired time and day, pause it, rewind it, forward it or can have the exactly same experience has viewing froma personalized DVD player. This is only possible because of the two-way communication between the set-top box and the server. In BSNL one has a choice of selecting from hundreds of movies while VOD offered by DTH providers may have only few movies to offer.

3.11 SET-TOP-BOX

The set-top box is a smart solid-state device that acts as the gateway to a host of services offered on the BSNL Multiplay network. On one side the set-top box interfaces with the television using the 3-RCA or the S-Video ports, and on the other side it is connected to broadband ADSL modem via the Ethernet port. BSNL franchisee in Pune has named the set-top box as WICE Box (Window for Information, Communication and Entertainment) and supports all sorts of inputs like audio, video, tablet data, text data, pointer devices etc. it has a USB port and a microphone and headphone jack in addition to essential ports. In future, it will be possible to connect keyboard, mouse, web cams, pen-drives and other such devices for various applications that will be provided on the box. The WICE box is fully upgradeable through the network. This means, any new application launched will be directly uploaded into WICE box without getting the box to the service center. All software upgrade will be handled this way.

3.12 VOIP

- The technology used to transmit voice conversations over a data networkusing the Internet Protocol.
- A category of hardware and software that enables people to use the Internetas the transmission medium for telephone calls.
- VoIP works through sending voice information in digital form in packets,
- VoIP also is referred to as Internet telephony, IP telephony, or Voice overthe Internet (VOI)

3.13 CONCLUSION

Broadband Multiplay network provides voice, data and video services, and hence called multiplay (Multiple Services). Major components CPE, DSLAM, RPR Switches, monitoring each and every packet and its quality parameters and accordingly provides services to end users.

4 IPV6

4.1 LEARNING OBJECTIVES

- Limitations Of IPv4
- IPv6 Address Presentation
- Features Of IPv6
- IPv6 Header Format
- IPv6 Prefixes & Types
- The IPv6 Interface Id And Eui-64 Format
- The IPv6 Address Hierarchy
- Multicast Ipv6 Address

4.1 INTRODUCTION

Internet Protocol version 6 (IPv6) is the sixth revision in the development of the Internet Protocol (IP) and the second version of the protocol to be widely deployed. Together with IPv4, it is at the core of standards-based internetworking methods of the Internet.

The current version of IP - IPv4 has not changed substantially since RFC 791, which was published in 1981. IPv4 has proven to be robust, easily implemented, and interoperable. It has stood up to the test of scaling an internetwork to a global utility the size of today's Internet. This is a tribute to its initial design.

However, the initial design of IPv4 did not anticipate the areas like growth of internet, need for simpler configuration, security consideration, support for prioritized and real-time delivery of data etc.

4.2 IPV4

- Limitations of IPv4
- Features of IPv6
- Uses of IPv6

4.3 LIMITATIONS OF IPV4

4.3.1 Addressing Problem

Although the 32-bit address space of IPv4 allows for 4.38 billion addresses, previous and current allocation practices limit the number of public IPv4 addresses to a few

hundred million. As a result, public IPv4 addresses have become relatively scarce, forcing many users and some organizations to use a NAT (Network Address Translation) to map a single public IPv4 address to multiple private IPv4 addresses.

Additionally, the rising prominence of Internet-connected devices and appliances ensures that the public IPv4 address space will eventually be depleted.

4.3.2 Routing Crises

Initially, IPv4 addressing scheme was following classful addressing. However, with the expansion of Internet and re-allocation of IPv4 address space, this classful addressing form lost its original shape and transformed into classless addressing by opting for options like subnetting and VLSM. This resulted in loss of aggregation of routes and routing entries have increased tremendously resulting in routing crises for the router for routing the traffic.

4.3.3 End To End Problem

As current IPv4 address space provides only a few hundred million public addresses, which are insufficient for fulfilling the need of hosts in the Internet world. In order to overcome this limitation, with the help of NAT, a single global address is being mapped with private address space. Although NATs promote reuse of the private address space, they violate the fundamental design principle of the original Internet that all nodes have a unique, globally reachable address, preventing true end-to-end connectivity for all types of networking applications.

4.3.4 Security

Private communication over a public medium such as the Internet requires cryptographic services that protect the data being sent from being viewed or modified in transit. Although a standard now exists for providing security for IPv4 packets (known as Internet Protocol security, or IPsec), this standard is optional for IPv4 and additional security solutions, some of which are proprietary, are prevalent.

4.3.5 Mobility

The problem of mobility for IPv4 was first addressed in a standards track specification, RFC 2002, “IP Mobility Support,” in 1996. But this mobility is limited in true sense.

4.3.6 Performance And Cost

The performance of IPv4 network will deteriorate if the infrastructure is not upgraded with time to match the traffic requirement which is increasing with application as well as user base along with routing entries because of increasing network complexity. This also involves cost in terms of trained man-power to maintain it. Also it requires efforts

for configuring services like NAT which is mainly because of scarcity of IPv4 resources.

4.4 IPV6 ADDRESS PRESENTATION

4.4.1 Ipv6 Address In Binary Form:

00100001110110100000000011010011000000000000000000010111100111011

00000010101010100000000011111111111111100010100010011100010110 10

4.4.2 Divided Into 8 Blocks Of 16 Bit

0010000111011010 0000000011010011 0000000000000000 0010111100111011

0000001010101010 0000000011111111 1111111000101000 1001110001011010

Each 16-bit block is converted to hexadecimal and separated with colons:

21DA : 00D3 : 0000 : 2F3B : 02AA : 00FF : FE28 : 9C5A

4.4.3 Suppression Of Zeros

Suppress leading zeros within each 16-bit block:

2000:1110 :1287 : 0003 : F7A9 : 00FF : FE14 : 7AD2

As 2000 :1110 :1287 : 3 : F7A9 : FF : FE14 : 7AD2

But trailing 0s cannot be removed as shown:

2000 : 1110 : 1287 : 3000 : F7A9 : FF00 : FE14 :7AD2

cannot be written as:

2000: 1110 : 1287 : 3 : F7A9 : FF : FE14 : 7AD2

4.4.4 Compression Of Zeros

All zeros in a 16 bit block can be represented by single zero

2345 : 0000 : 0000 : 0000 : 0000 : 1234 : 3458 : AC19

can be represented as :

2345 : 0 : 0 : 0 : 0 : 1234 : 3458 : C19

An Address having more than one zeros can be represented as double colon ::

(Double Colon)

2345 : 0 : 0 : 0 : 0 : 1234 : 3458 : C19

becomes 2345 :: 1234 : 3458 : C19

FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 2 becomes FF02::2

0 : 0 : 0 : 0 : 0 : 0 : 0 : 1 becomes ::1

FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 0 becomes FF02 ::

Double colon :: can be used only once in an address.

2001 : 0 : 0 : 0 : 1234 : 0 : 0 : C1C0

can be written as

2001 :: 1234 : 0 : 0 : C1C0

Or 2001 : 0 : 0 : 0 : 1234 :: C1C0

but not as 2001 :: 1234 :: C1C0

4.5 FEATURES OF IPV6

4.5.1 Large Address Space

IPv6 has 128-bit (16-byte) addresses. Although 128 bits can express over 3.4 × 1038 possible combinations, the large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation, from the Internet backbone to the individual subnets within an organization.

Even with all of the addresses currently assigned for use by hosts, plenty of addresses are available for future use. With a much larger number of available addresses, address-conservation techniques, such as the deployment of NATs, are no longer necessary.

4.5.2 Global Reachability

With IPv4 NATs, there is a technical barrier for applications that rely on listening or peer based connectivity because of the need for the communicating peers to discover and advertise their public IPv4 addresses and ports.

With IPv6, NATs are no longer necessary to conserve public address space, and the problems associated with mapping addresses and ports disappear for developers of applications and gateways. More importantly, end-to-end communication is restored between hosts on the Internet by using addresses in packets that do not change in transit. This functional restoration has immense value when one considers the emergence of peer-to-peer telephony, video, and other real-time collaboration technologies for personal communications etc.

By restoring global addressing and end-to-end connectivity, IPv6 has no barrier to new applications that are based on ad hoc connectivity and peer-based communication.

4.5.3 Scoped Address And Address Selection

Unlike IPv4 addresses, IPv6 addresses have a scope, or a defined area of the network over which they are unique and relevant. For example, IPv6 has a global address that is equivalent to the IPv4 public address and a unique local address that is roughly equivalent to the IPv4 private address. Typical IPv4 routers do not distinguish a public address from a private address and will forward a privately addressed packet on the Internet. An IPv6 router, on the other hand, is aware of the scope of IPv6 addresses and will never forward a packet over an interface that does not have the correct scope.

There are different types of IPv6 addresses with different scopes. When multiple IPv6 addresses are returned in a DNS name query, the sending node must be able to distinguish their types and, when initiating communication, use a pair (source address and destination address) that is matched in scope and that is the most appropriate pair to use. For example, for a source and a destination that have been assigned both global (public) and link-local addresses, a sending IPv6 host would never use a global destination with a link-local source. IPv6 sending hosts include the address selection logic that is needed to decide which pair of addresses to use in communication. Moreover, the address selection rules are configurable.

This allows you to configure multiple addressing infrastructures within an organization. Regardless of how many types of addressing infrastructures are in place, the sending host always chooses the “best” set of addresses. In comparison, IPv4 nodes have no awareness of address types and can send traffic to a public address from a private address.

The benefit of scoped addresses is that by using the set of addresses of the smallest scope, your traffic does not travel beyond the scope for the address, exposing your network traffic to fewer possible malicious hosts.

4.5.4 New Header Format

The IPv6 header has a new format that is designed to minimize header processing. This is achieved by moving both nonessential and optional fields to extension headers that are placed after the IPv6 header. The streamlined IPv6 header is more efficiently processed at intermediate routers.

IPv4 headers and IPv6 headers are not interoperable. IPv6 is not a superset of functionality that is backward compatible with IPv4.

Implementation of both IPv4 and IPv6 to recognize and process both header formats. The new default IPv6 header is only twice the size of the default IPv4 header, even though the number of bits in IPv6 addresses is four times larger than IPv4 addresses.

4.5.5 Stateless And Stateful Address Configuration

To simplify host configuration, IPv6 supports both stateful address configuration (such as address configuration in the presence of a DHCP for IPv6) and stateless address configuration (such as address configuration in the absence of a DHCPv6 server).

With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses), with IPv6 transition addresses, and with addresses derived from prefixes advertised by local routers.

4.5.6 Ipsec Header Support Required

Support for the IPsec headers is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network protection needs and promotes interoperability between different IPv6 implementations. IPsec consists of two types of extension headers and a protocol to negotiate security settings. The Authentication header (AH) provides data integrity, data authentication, and replay protection for the entire IPv6 packet (excluding fields in the IPv6 header that must change in transit). The Encapsulating Security Payload (ESP) header and trailer provide data integrity, data authentication, data confidentiality, and replay protection for the ESP-encapsulated payload.

4.5.7 Better Support For Prioritized Delivery

New fields in the IPv6 header define how traffic is handled and identified. Traffic is prioritized using a Traffic Class field, which specifies a DSCP value just like IPv4. A Flow Label field in the IPv6 header allows routers to identify and provide special handling for packets that belong to a flow (a series of packets between a source and destination). Because the traffic is identified in the IPv6 header, support for prioritized delivery can be achieved even when the packet payload is encrypted with IPsec and ESP.

4.5.8 New Protocol For Neighboring Node Interaction

The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manages the interaction of neighboring nodes (nodes on the same link). Neighbor Discovery replaces and extends the Address Resolution Protocol (ARP) (broadcast-based), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages.

4.5.9 Extensibility

IPv6 can easily be extended for new features by adding extension headers after the IPv6 header. Unlike options in the IPv4 header, which can support only 40 bytes of options, the size of IPv6 extension headers is constrained only by the size of the IPv6 packet.

4.5.10 Efficient Forwarding

IPv6 is a streamlined version of IPv4. Excluding prioritized delivery traffic, IPv6 has fewer fields to process and fewer decisions to make in forwarding an IPv6 packet. Unlike IPv4, the IPv6 header is a fixed size (40 bytes), which allows routers to process IPv6 packets faster.

Additionally, the hierarchical and summarizable addressing structure of IPv6 global addresses means that there are fewer routes to analyze in the routing tables of organization and Internet backbone routers. The consequence is traffic that can be forwarded at higher data rates, resulting in higher perforance for tomorrow's high-bandwidth applications that use multiple data types.

4.5.11 Support For Security And Mobility

IPv6 has been designed to support security (IPsec) (AH and ESP header support required) and mobility (Mobile IPv6) (optional). Although one could argue that these features are available for IPv4, they are available on IPv4 as extensions, and therefore they have architectural or connectivity limitations that might not have been present if they had been part of the original IPv4 design. It is always better to design features in rather than bolt them on. The result of designing IPv6 with security and mobility in mind is an implementation that is a defined standard, has fewer limitations, and is more robust and scalable to handle the current and future communication needs of the users of the Internet.

The business benefit of requiring support for IPsec and using a single, global address space is that IPv6 can protect packets from end to end across the entire IPv6 Internet. Unlike IPsec on the IPv4 Internet, which must be modified and has limited functionality when the endpoints are behind NATs, IPsec on the IPv6 Internet is fully functional between any two endpoints.

4.6 IPV6 HEADER FORMAT

The format of the IPv6 packet header is simplified from its counterpart in IPv4. The length of the IPv6 header increases to 40 bytes (from 20 bytes) and contains two 16-byte addresses (source and destination), preceded by 8 bytes of control information, as shown in Figure.

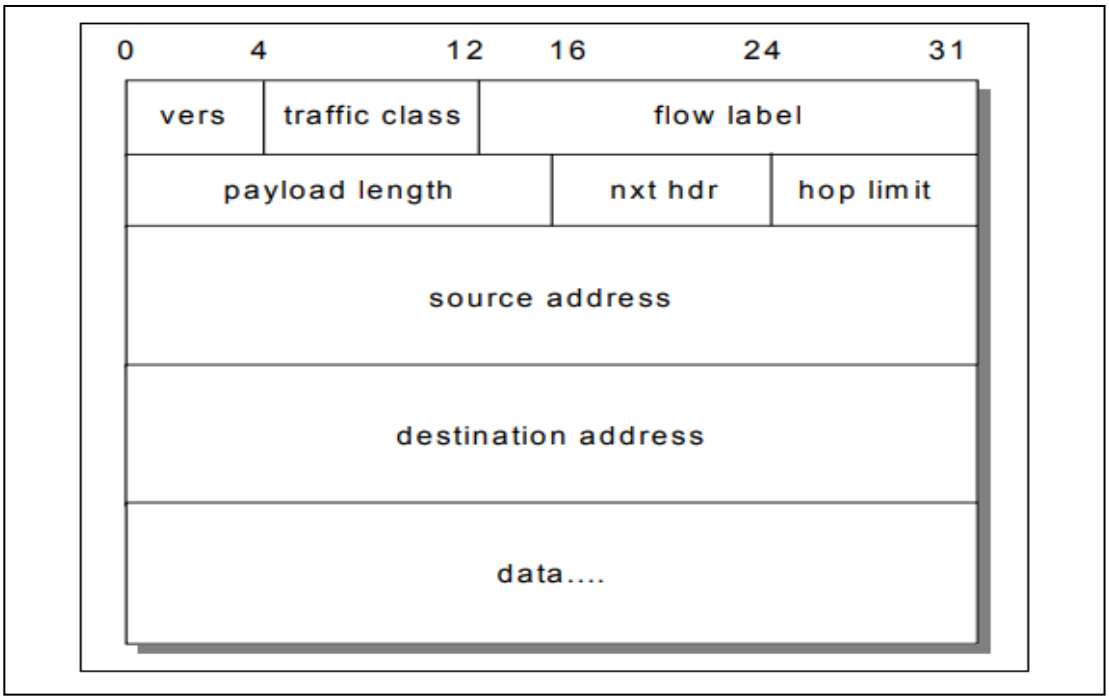


Figure 24: **Header format**

The IPv4 header has two 4-byte addresses preceded by 12 bytes of control information and possibly followed by option data. The reduction of the control information and the elimination of options in the header for most IP packets optimizes the processing time per packet in a router. The infrequently used fields removed from the header are moved to optional extension headers when they are required.

The IPv6 header has 8 fields and is 320 bits long. It has been considerably streamlined compared to its IPv4 counterpart, which has 12 fields and is 160 bits long.

Field	**Length**	**Description**
Version	4 bits	Version of IP (in this case, IPv6)
Traffic Class	8 bits	Classifies traffic for QoS
Flow Label	20 bits	Identifies a flow between a source and destination
Payload Length	16 bits	Length of data in packet

Next Header	8 bits	Specifies the next upper-layer or extension header
Hop Limit	8 bits	Decremented by each router traversed
Source Address	128 bits	Source IPv6 address
Destination Address	128 bits	Destination IPv6 address

Table 2. IPv6 Headers

The Next Header field is of some importance. This field can identify either the next upper-layer header (for example, UDP, TCP or ICMP), or it can identify a special Extension Header, which is placed in between the IPv6 and upper layer header.

Several such extension headers exist, and are usually processed in the following order:

Hop-by-Hop Options – specifies options that should be processed by every router in the path. Directly follows the IPv6 header.

Destination Options – specifies options that should be processed by the destination device.

Routing Header – specifies each router the packet must traverse to reach the destination (source routing)

Fragment Header – used when a packet is larger than the MTU for the path

Authentication Header – used to integrate IPSEC Authentication Header (AH) into the IPv6 packet

ESP Header – used to integrate IPSEC Encapsulating Security Payload (ESP) into the IPv6 packet

4.7 IPV6 PREFIXES & TYPES OF IPV6

Prefix is the part of the address where the bits have fixed values or are the bits of a route or subnet identifier.

Prefixes for IPv6 subnet identifiers, routes, and address ranges are expressed in the same way as Classless Inter-Domain Routing (CIDR) notation for IPv4.

An IPv6 prefix is written in address/prefix-length notation.

Examples:

21DA:D3::/48 for a route

21DA:D3:0:2F3B::/64 for a subnet

No more dotted decimal subnet masks

Typical unicast IPv6 address:

64 bits for subnet ID, 64 bits for interface ID

Full Address: 1254:1532:26B1:CC14:123:1111:2222:3333/64

Prefix ID: 1254:1532:26B1:CC14:

Host ID: 123:1111:2222:3333

The /64 indicates that the first 64 bits of this address identify the prefix.

4.8 THE IPV6 INTERFACE ID AND EUI-64 FORMAT

The host portion of an IPv4 address is not based on the hardware address of an interface. IPv4 relies on **Address Resolution Protocol (ARP)** to map between the logical IP address and the **48-bit** hardware **MAC address**.

IPv6 unicasts generally allocate the first 64 bits of the address to identify the network (**prefix**), and the last 64 bits to identify the host (referred to as the **interface ID**). The interface ID *is* based on the interface's hardware address.

This interface ID adheres to the IEEE **64-bit Extended Unique Identifier** (**EUI-64**) format. Since most interfaces still use the 48-bit MAC address, the MAC must be converted into the EUI-64 format.

Consider the following MAC address: 1111.2222.3333. The first 24 bits, the Organizationally Unique Identifier (OUI), identify the manufacturer. The last 24 bits uniquely identify the host. To convert this to EUI-64 format:

1. The **first 24 bits** of the MAC **(**the **OUI**), become the first 24 bits of the EUI-64 formatted interface ID.
2. The ***seventh*** bit of the OUI is changed from a "**0**" to a "**1**".
3. The next 16 bits of the interface ID are **FFFE.**
4. The **last 24 bits** of the MAC (the **host ID**), become the last 24 bits of the interface ID.

Thus, the MAC address 1111.2222.3333 in EUI-64 format would become

1311:22FF:FE22:3333, which becomes the interface ID.

4.9 THE IPV6 ADDRESS HIERARCHY

IPv4 separated its address space into specific **classes.** The class of an IPv4 address was identified by the high-order bits of the first octet:

- **Class A** - (00000001 – 01111111, or 1 - 127)
- **Class B** - (10000000 – 10111111, or 128 - 191)
- **Class C** - (11000000 – 11011111, or 192 - 223)
- **Class D** - (11100000 – 11101111, or 224 - 239)

IPv6's addressing structure is far more scalable. Less than 20% of the IPv6 address space has been designated for use, currently. The potential for growth is enormous.

The address space that *has* been allocated is organized into several types, determined by the high-order bits of the first field:

- **Special Addresses –** addresses begin **00*xx*:**
- **Link Local –** addresses begin **FE8*x*:**
- **Site Local –** addresses begin **FEC*x*:**
- **Aggregate Global –** addresses begin **2*xxx*:** or **3*xxx*:**
- **Multicasts –** addresses begin **FF*xx*:**
- **Anycasts**

(Note: an "x" indicates the value can be any hexadecimal number)

There are **no broadcast addresses** in IPv6. Thus, any IPv6 address that is not a *multicast* is a *unicast* address.

Anycast addresses identify a group of interfaces on multiple hosts. Thus, multiple hosts are configured with an *identical* address. Packets sent to an anycast address are sent to the *nearest* (i.e., least amount of hops) host.

Anycasts are indistinguishable from any other IPv6 unicast address.

Practical applications of anycast addressing are a bit murky. One possible application would be a server farm providing an identical service or function, in which case anycast addressing would allow clients to connect to the nearest server.

4.10 SPECIAL (RESERVED) IPV6 ADDRESSES

The first field of a **reserved** or **special** IPv6 address will always begin **00*xx*.**

Reserved addresses represent 1/256th of the available IPv6 address space. Various reserved addresses exist, including:

- **0:0:0:0:0:0:0:0** (or **::**) – is an **unspecified** or **unknown** address.
  It is the equivalent of the IPv4 0.0.0.0 address, which indicates

the absence of a configured or assigned address. In routing tables, the unspecified address is used to identify **all** or **any** possible hosts or networks.

- **0:0:0:0:0:0:0:1 (**or **::1**) – is the **loopback** or **localhost** address. It is the equivalent of the IPv4 127.0.0.1 address.

4.11 RESERVED ADDRESSES - IPV4 AND IPV6 COMPATIBILITY

To alleviate the difficulties of immediately migrating from IPv4 to IPv6, specific reserved addresses can be used to *embed* an IPv4 address into an IPv6 address.

Two types of addresses can be used for IPv4 embedding, **IPv4-compatible IPv6 addresses**, and **IPv4-mapped IPv6 addresses**.

- **0:0:0:0:0:0:a.b.c.d (**or **::a.b.c.d)** – is an **IPv4-compatible IPv6 address**. This address is used on devices that support both IPv4 and IPv6. A prefix of /96 is used for IPv4-compatible IPv6 addresses:

  ::192.168.1.1/96

- **0:0:0:0:0:FFFF:a.b.c.d** (or **::FFFF:a.b.c.d) –** is an **IPv4-mapped IPv6 address.** This address is used by IPv6 routers and devices to identify non-IPv6 capable devices. Again, a prefix of /96 is used for IPv4-mapped IPv6 addresses:
  ::FFFF:192.168.1.1/96

4.12 LINK-LOCAL IPV6 ADDRESSES

Link-local IPv6 addresses are used only on a single link (subnet). Any packet that contains a link-local source or destination address is *never routed* to another link. Every IPv6-enabled interface on a host (or router) is assigned a link-local address. This address can be manually assigned, or auto-configured.

The first field of a link-local IPv6 address will always begin FE8x (1111 1110 10). Link-local addresses are unicasts, and represent 1/1024th of the available IPv6 address space. A prefix of /10 is used for link-local addresses.

FE80::1311:22FF:FE22:3333/10

There is no hierarchy to a link-local address:

- The first 10 bits are fixed (**FE8**), known as the **Format Prefix (FP).**

- The next 54 bits are set to **0.**
- The final 64 bits are used as the **interface ID**.

4.13 SITE LOCAL IPV6 ADDRESSES

Site-local IPv6 addresses are the equivalent of "private" IPv4 addresses. Site-local addresses can be routed within a *site* or *organization*, but cannot be globally routed on the Internet. Multiple private subnets within a "site" are allowed.

The first field of a **site-local** IPv6 address will always begin **FECx (1111 1110 11).** Site-local addresses are **unicasts,** and represent 1/1024th of the available IPv6 address space.

FEC0::2731:E2FF:FE96:C283/64

Site-local addresses do adhere to a hierarchy:

- The first 10 bits are the fixed FP (**FEC**).
- The next 38 bits are set to **0.**
- The next 16 bits are used to identify the **private subnet ID**.
- The final 64 bits are used as the **interface ID**. To identify two separate subnets (1111 and 2222):

FEC0::1111:2731:E2FF:FE96:C283/64
FEC0::2222:97A4:E2FF:FE1C:E2D1/64

4.14 AGGREGATE GLOBAL IPV6 ADDRESSES

Aggregate Global IPv6 addresses are the equivalent of "public" IPv4 addresses. Aggregate global addresses can be routed publicly on the Internet. Any device or site that wishes to traverse the Internet must be uniquely identified with an aggregate global address.

Currently, the first field of an **aggregate global** IPv6 address will always begin **2*xxx* (001).** Aggregate global addresses are **unicasts,** and represent 1/8th of the available IPv6 address space.

2001::2731:E2FF:FE96:C283/64

Aggregate global addresses adhere to a very strict hierarchy:

- The first 3 bits are the fixed FP.
- The next 13 bits are the **top-level aggregation identifier (TLA ID).**
- The next 8 bits are **reserved** for future use.

- The next 24 bits are the **next-level aggregation identifier (NLA ID).**
- The next 16 bits are the **site-level aggregation identifier (SLA ID).**
- The final 64 bits are used as the **interface ID**.

By have multiple **levels**, a consistent, organized, and scalable hierarchy is maintained. High level registries are assigned ranges of TLA IDs. These can then be subdivided in the NLA ID field, and passed on to lower-tiered ISPs.

Such ISPs allocate these prefixes to their customers, which can further subdivide the prefix using the SLA ID field, to create whatever local hierarchy they wish. The 16-bit SLA field provides up to 65535 networks for an organization.

Note: Do not confuse the SLA ID field of a global address field, with a site- local address. Site-local addresses cannot be routed publicly, where as SLA ID's are just a subset of the publicly routable aggregate global address.

4.15 MULTICAST IPV6 ADDRESSES

Multicast IPv6 addresses are the equivalent of IPv4 multicast addresses. Interfaces can belong to one or more multicast **groups**. Interfaces will accept a multicast packet only if they belong to that group. Multicasting provides a much more efficient mechanism than **broadcasting**, which requires that every host on a link accept and process each broadcast packet.

The first field of a **multicast** IPv6 address will always begin **FF*xx* (1111 1111).** The full multicast range is **FF00** through **FFFF**. **Multicasts** represent 1/256th of the available IPv6 address space.

FF01:0:0:0:0:0:0:1

Multicast addresses follow a specific format:

- The first 8 bits **identify the address** as a **multicast** (1111 1111)
- The next 4 bits are a **flag value**. If the flag is set to all zeroes (0000), the multicast address is considered *well-known*.
- The next 4 bits are a **scope value**:
  - 0000 (0) = Reserved
  - 0001 (1) = Node Local Scope
  - 0010 (2) = Link Local Scope
  - 0101 (5) = Site Local Scope
  - 1000 (8) = Organization Local Scope
  - 1110 (e) = Global Scope
  - 1111 (f) = Reserved
- The final 112 bits identify the actual **multicast group**.

IPv4 multicast addresses had no mechanism to support multiple "**scopes.**" IPv6 scopes allow for a multicast hierarchy, a way to *contain* multicast traffic.

4.16 COMMON IPV6 MULTICAST ADDRESSES

The following is a list of common, well-known IPv6 multicast addresses:

Node-Local Scope Multicast Addresses

- FF01::1 – All-nodes address
- FF01::2 – All-routers address

Link-Local Scope Multicast Addresses

- FF02::1 – All-nodes address
- FF02::2 – All-routers address
- FF02::5 – OSPFv3 (OSPF IPv6) All SPF Routers
- FF02::6 – OSPFv3 Designated Routers
- FF02::9 – RIPng Routers
- FF02::13 – PIM Routers

Site-Local Scope Multicast Addresses

- FF05::2 – All-routers address

All hosts must join the **all-nodes** multicast group, for both the node-local and link-local scopes. All routers must join the **all-routers** multicast group, for the node-local, link-local, and site-local scopes.

Every site-local and aggregate global address is assigned a **solicited-node multicast** address. This solicited-node address is created by appending the last 24 bits of the interface ID to the following prefix: FF02::1:FF/103.

Thus, if you have a site-local address of:

FEC0::1111:2731:E2FF:FE96:C283

The corresponding solicited-node multicast address would be:

FF02::1:FF96:C283

Solicited-node multicast addresses are most often used for neighbor discovery (covered in an upcoming section in this guide).

4.17 REQUIRED IPV6 ADDRESSES

At a minimum, each IPv6 interface on a **host** must recognize the following IPv6 addresses:

- The loopback address
- A link-local address
- Any configured site-local or aggregate global addresses
- Any configured multicast groups
- The all-nodes multicast address (both node-local and link-local scopes)
- The solicited-node multicast address for any configured unicast addresses

In addition to the above addresses, each IPv6 interface on a **router** must recognize the following IPv6 addresses:

- The subnet-router anycast address
- Any configured multicast groups
- The all-routers multicast address (node-local, link-local, and site-local scopes)

4.18 CONCLUSION

There are many reasons for IPv6 supports and there is also need to migrate from current version of Internet IPv4 to IPv6 for availing additional benefits of Internet. However, for quite some time, things will move in parallel and smooth transition will be in benefit for the Internet world. Therefore, we will see IPv4 and IPv6 simultaneously being used by the Internet users, and the service provider. Also the application that will be developed during this phase will also keep in mind the requirement of IPv4 and IPv6.

5 MPLS VPN

5.1 LEARNING OBJECTIVES

- Drawbacks Of Traditional IP Forwarding
- MPLS Advantages
- MPLS Header
- Various Routing Function Units & Routers In MPLS
- MPLS Operation
- MPLS Router Functionality
- Label Distribution And Forwarding Of Packets
- Label Distribution Protocol
- MPLS VPN – Overlay And Peer To Peer Model
- MPLS Architecture

5.2 INTRODUCTION

Multi Protocol Label Switching (MPLS) is an efficient encapsulation mechanism that uses “Labels” appended to packets (IP packets, AAL5 frames) for transport of data. MPLS packets can run on other layer 2 technologies such as ATM, FR, PPP, POS, Ethernet. Other layer 2 technologies can be run over an MPLS network. Labels can be used as designators. For example—IP prefixes, ATM VC, or a bandwidth guaranteed path.

It operates at a layer that is generally considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer or IP Layer), and thus MPLS is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients, which provide a data-gram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, Frame relay and Ethernet frames. The IP network has emerged as the network for providing converged, differentiated classed of services to user with optimal use of resources and also to address the issues related to Class of service (CoS) and Quality of Service (QoS). MPLS is the technology that addresses all the issues in the most efficient manner. MPLS is a packet-forwarding technology that uses labels to make data forwarding decisions.

5.3 DRAWBACKS OF TRADITIONAL IP FORWARDING

- Routing protocols are used to distribute Layer 3 routing information and therefore every router may need full Internet routing information (more than 100,000 routes).

- Forwarding is based on the destination address only.
- Routing lookups are performed on every hop that slows down the forwarding operation.
- Packets can't be given priority. Though TOS field is there in IP packets through which priority can be given to packets but routers are designed to bypass the TOS field.
- Layer 2 devices have no knowledge of Layer 3 routing information —virtual circuits must be manually established.

5.4 MPLS ADVANTAGES

1. Specifies mechanisms to manage traffic flow of various granularities, such as flows between different hardware, machines, or even flows between different applications.
2. Create new services via flexible classification
3. Provides the ability to setup bandwidth guaranteed paths
4. Enable ATM switches to act as routers
5. MPLS remains independent of the Layer-2 & layer-3 protocols. Meaning thereby that label encapsulating the data packet does not depend upon layer 3 /layer 2 protocol of data. This justifies the name as multi protocol label switching.
6. Provides a means to map IP addresses to simple, fixed-length labels used by different packet-forwarding and packet-switching technologies
7. Interfaces to existing routing protocols such as resource reservation protocol (RSVP) and open shortest path first (OSPF).
8. Supports the IP, ATM, and frame- relay Layer-2 protocols.
9. MPLS gives network operators a great deal of flexibility to divert and route traffic around linkfailures, congestion, and bottlenecks.
10. From a Quality of Service (QoS) standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss.
11. Enable ATM switches to act as routers

5.5 MPLS HEADER

5.5.1 What Is A MPLS Header?

MPLS works by prefixing packets with an MPLS header containing one or more 'labels'.

This is called a label stack. Each label stack entry contains four fields: -

- 20-bit label value (This is MPLS Label)
- 3-bit Experimental field used normally for providing for QoS (Quality of Service)
- 1-bit bottom of stack flag. If this is 1, signifies that the current label is the last in the stack.

- 8-bit TTL (time to live) field.

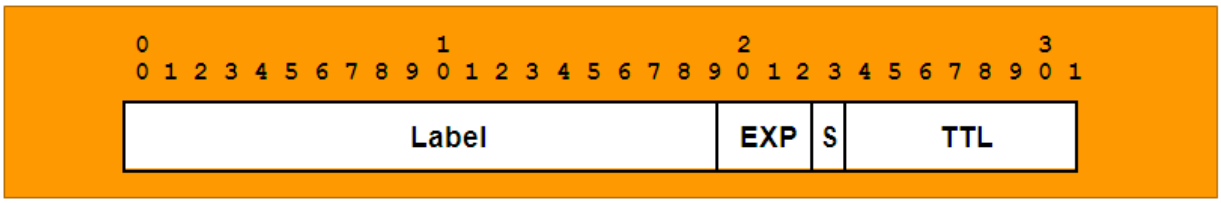


Figure 25: **MPLS Header format**

5.5.2 MPLS Label Stack

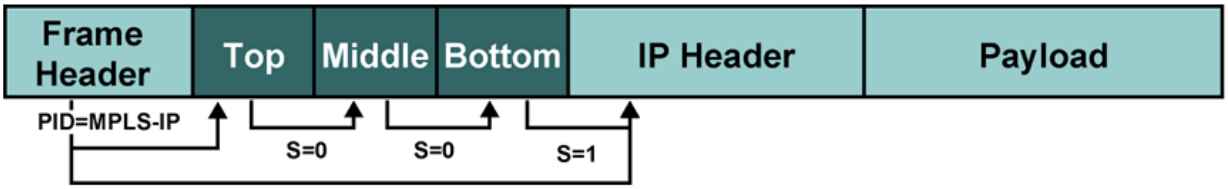


Figure 26: **MPLS label stack**

- Protocol identifier in a Layer 2 header specifies that the payload starts with a label (labels) and is followedby an IP header.
- Bottom-of-stack bit indicates whether the next header is another label or a Layer 3 header.
- Receiving router uses the top label only.
- Usually only one label is assigned to a packet.
- The following scenarios may produce more thanone label:
  - MPLS VPNs (two labels: The top label points to the egressrouter and the second label identifies the VPN.)
  - MPLS TE (two or more labels: The top label points to the endpoint of the traffic engineering tunnel and the second label points to the destination.)
  - MPLS VPNs combined with MPLS TE (three or more labels.)

5.6 VARIOUS ROUTING FUNCTION UNITS & ROUTERS IN MPLS

Routing function in MPLS can be described on the basis of some units, which are defined as follows:

Label: A label is an identifier, which indicates the path a packet, should traverse. Label is carried along with the packet. The receiving router examines the packet for its label content to determine the next hop. Once a packet has been labeled, the rest of the journey of the packet through the backbone is based on label switching. Since every intermediate

router has to look in to the label for routing the decision making at the level of the router becomes fast.

Label Creation: Every entry in the routing table (build by using any IGP protocol) is assigned a unique 20-bit label.

SWAP: Every incoming label is replaced by a new outgoing label (As per the path to be followed) and the packet is forwarded along the path associated with the new label.

PUSH: A new label is pushed on top of the packet, effectively "encapsulating" the original IP packet in a layer of MPLS.

POP: The label is removed from the packet effectively "de-encapsulating". If the popped label was the last on the label stack, the packet "leaves" the MPLS tunnel.

LER: A router that operates at the edge of the access network and MPLS network LER performs the PUSH and POP functions and is also the interface between access and MPLS network, commonly known as **Edge** router.

LSR: An LSR is a high-speed router device in the core of an MPLS network, normally called Core routers. These routers perform swapping functions and participate in the establishment of Label Switch Path (LSP)

Ingress / Egress Routers: The routers receiving the incoming traffic or performing the first PUSH function are ingress routers and routers receiving the terminating traffic or performing the POP function are Egress routers. The same router performs both functionality i.e. Ingress and Egress. The routers performing these functions are LER.

FEC: The forward equivalence class (FEC) is a representation of a group of packets that share the same requirements for their transport. All packets in such a group are provided the same treatment en route to the destination. As opposed to conventional IP forwarding, in MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network at the edge router.

5.7 BASIC MPLS OPERATION

When packets enter a MPLS-based network, **Label Edge Routers (LERs)** give them one or more labels (identifiers). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service.

Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets. With these LSPs, network operators can divert and route traffic based on data-streamtype and Internet-access customer

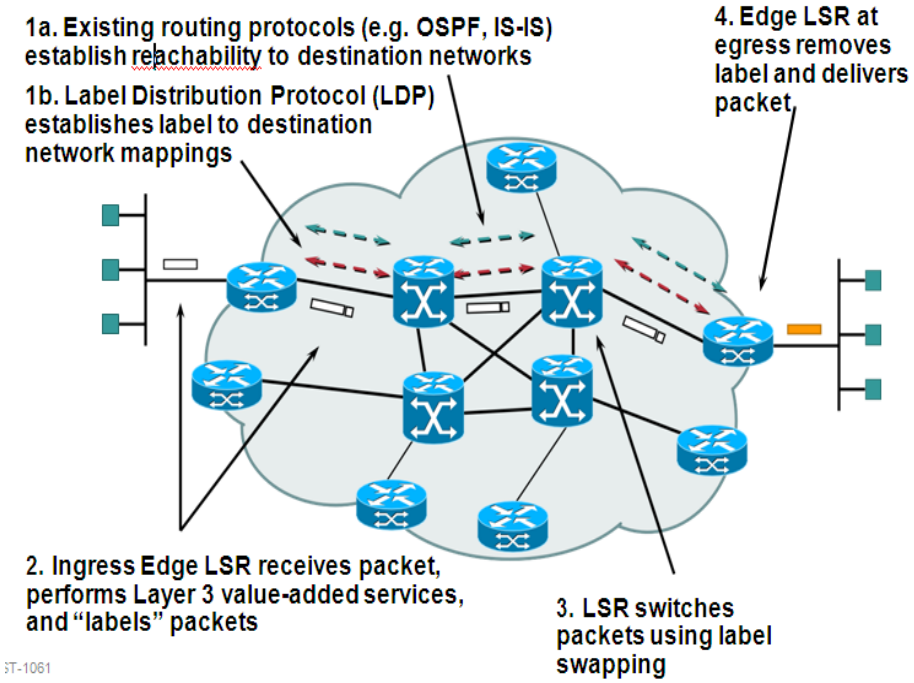


Figure 27: **MPLS operation**

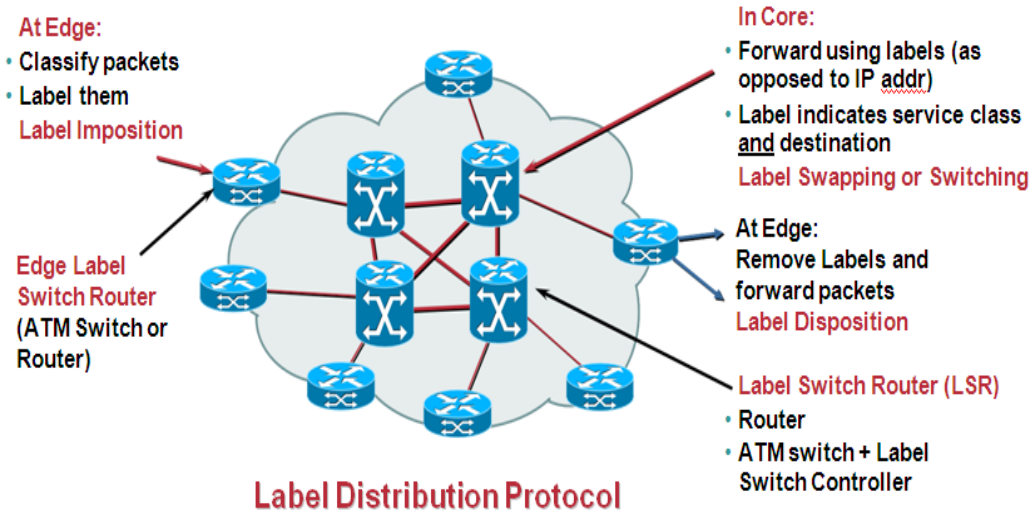


Figure 28: **Label distribution protocol**

The following steps must be taken for a data packet to travel through an MPLS domain:

- Label creation and distribution
- Table creation at each router
- Label-switched path creation
- Label insertion/table lookup
- Packet forwarding.

5.8 MPLS ROUTER FUNCTIONALITY

MPLS Router functionality is divided into two major parts

Control plane: Exchanges Layer 3 routinginformation and labels. Control plane contains complex mechanisms to exchange routing information, such as OSPF, EIGRP, IS-IS, and BGP, and to exchange labels, such as TDP,LDP, BGP, and RSVP.

Data plane: Forwards packets based on labels. Data plane has a simple forwarding engine.

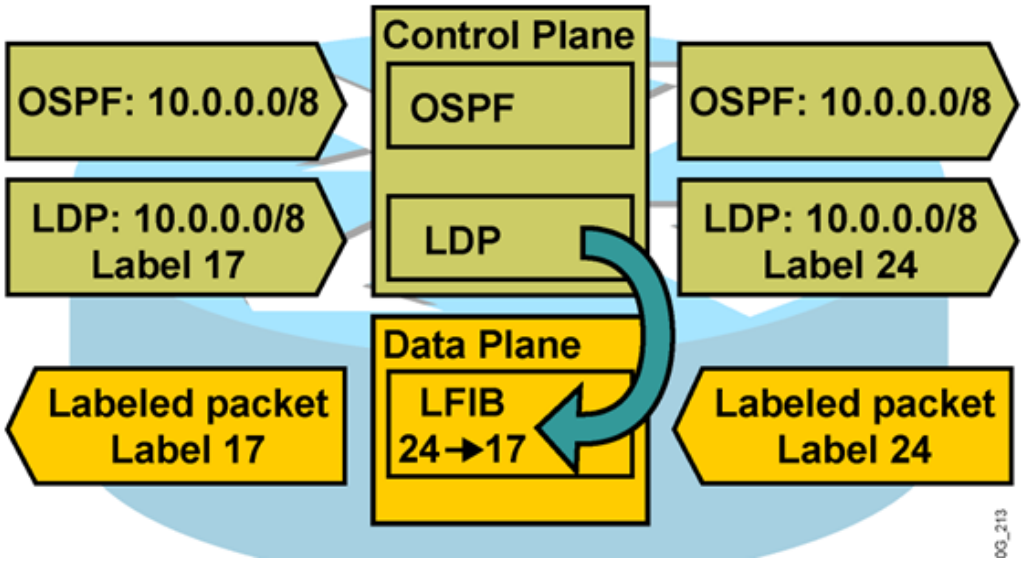


Figure 29: **MPLS Control and Data Plane Functionality**

Architecture of LER:

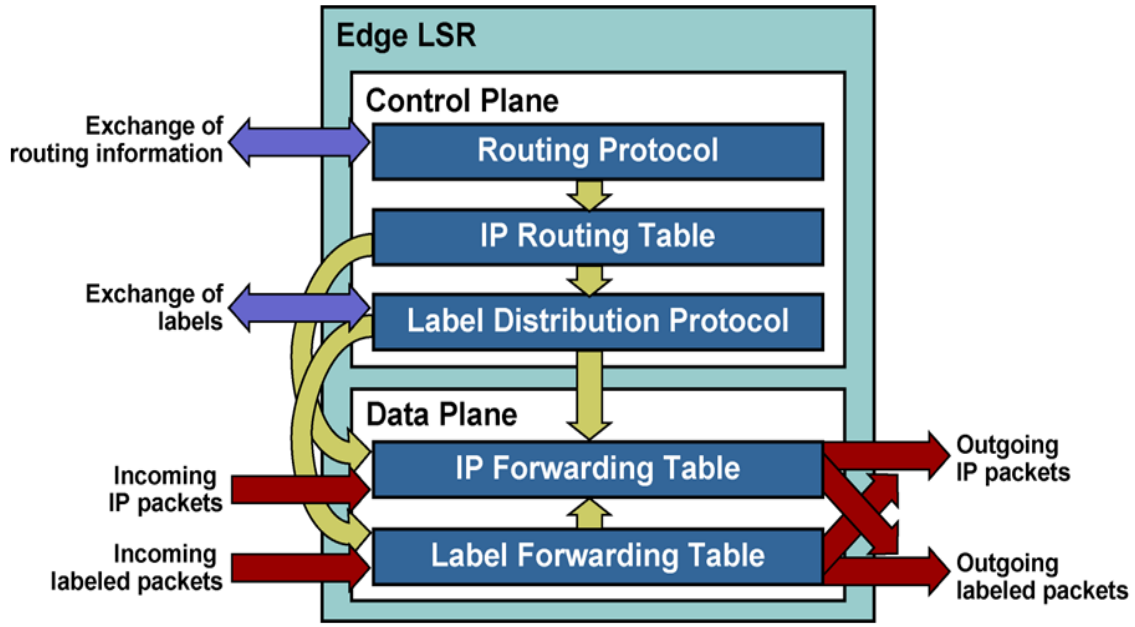


Figure 30: **LER architecture**

Architecture of LSR:

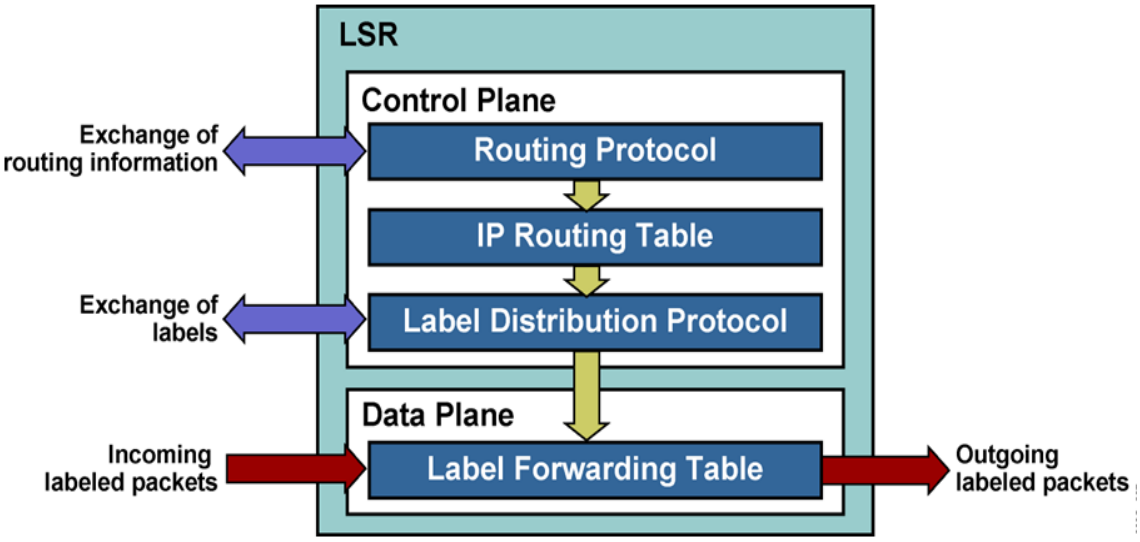


Figure 31: **LSR architecture**

5.9 LABEL DISTRIBUTION AND FORWARDING OF PACKETS IN MPLS NETWORKS

- OSPF, IS-IS, BGP are needed in the network
- They provide reachability

- Label distribution protocols distribute labels for - prefixes advertised by

unicast routing protocols using Either a dedicated Label Distribution Protocol (LDP, Extending existing protocols like BGP to distribute Labels

- Defined in RFC 3035 and 3036.
- It is used to distribute Labels in a MPLS network, Forwarding Equivalence Class(How packets are mapped to LSPs (Label Switched Paths)), Advertise Labels per FEC, Reach destination a.b.c.d with label x and Discovery

5.9.1 Router Example: Forwarding Packets

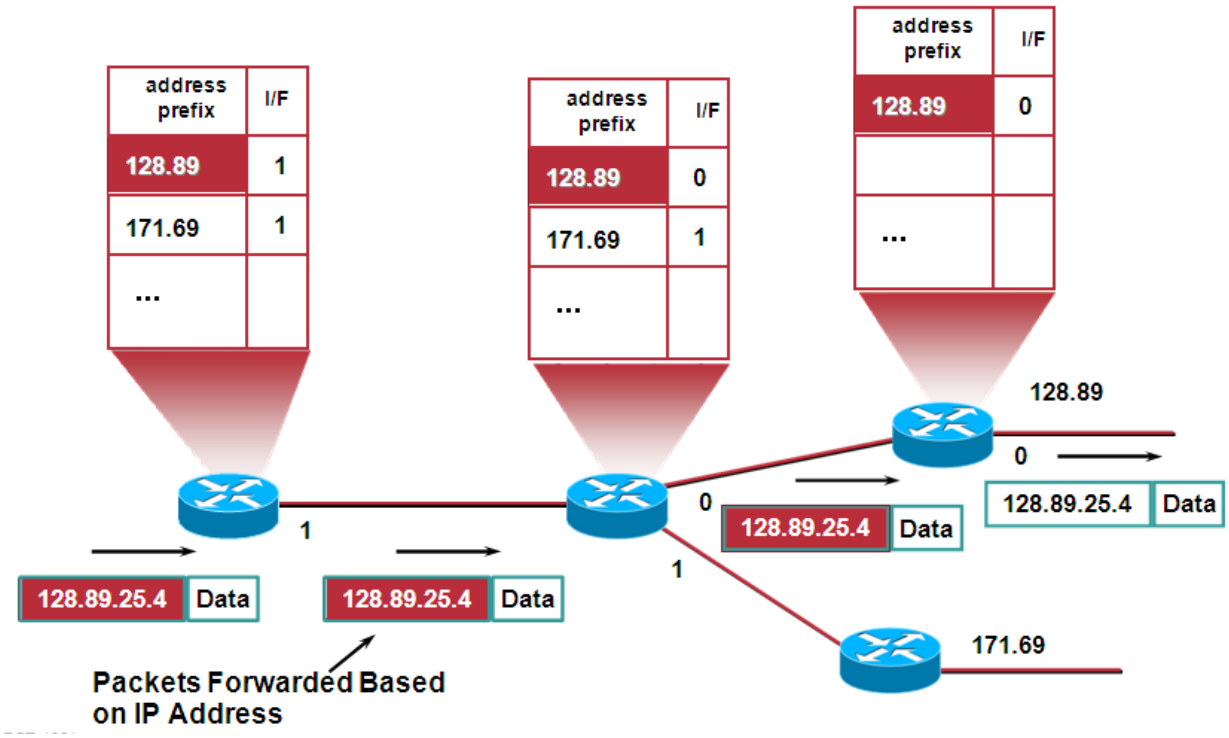


Figure 32: **Forwarding packets**

5.9.2 MPLS Example: Routing Information

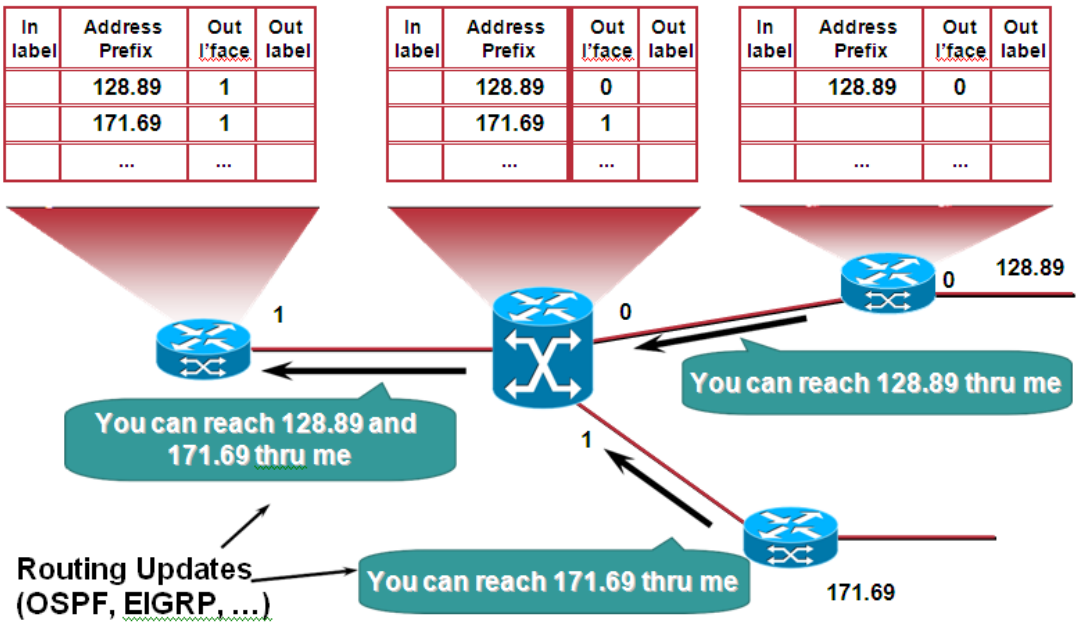


Figure 33: **Routing information**

5.9.3 MPLS Example: Assigning Labels

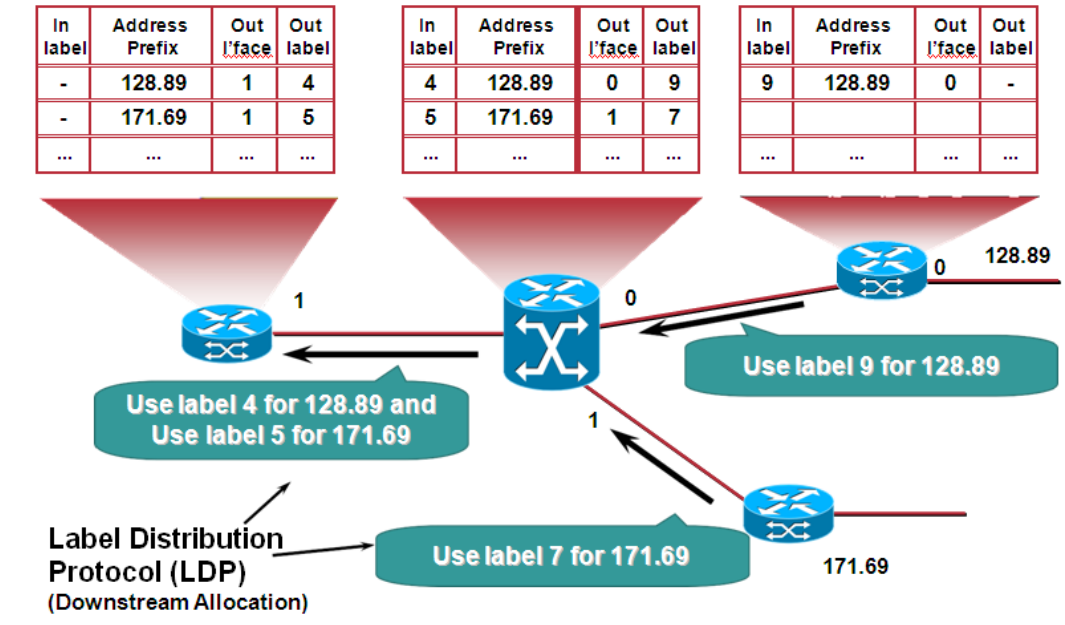


Figure 34: **Assigning labels**

5.9.4 MPLS Example: Forwarding Packets

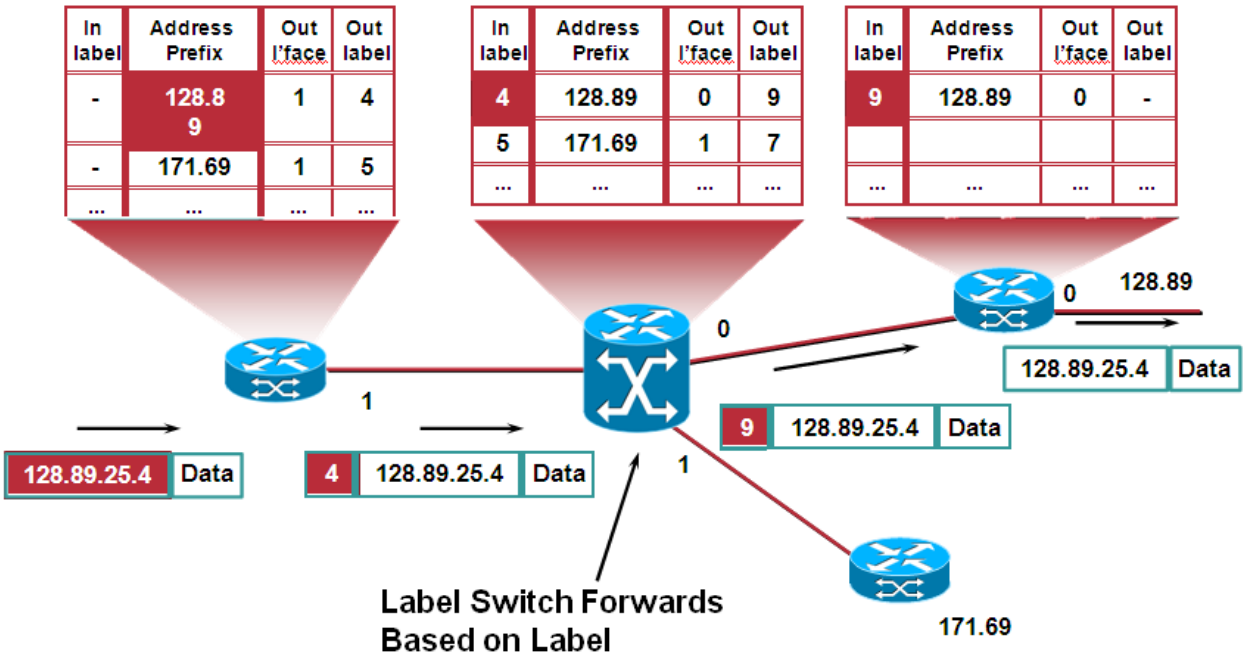


Figure 35: **Forwarding packets**

5.10 MPLS LABEL DISTRIBUTION PROTOCOLS

MPLS architecture does not mandate a single method of signaling for label distribution. Existing routing protocols, such as the border gateway protocol (BGP), have been enhanced to piggyback the label information within the contents of the protocol. The RSVP has also been extended to support piggybacked exchange of labels. A summary of the various schemes for label exchange isas follows:

- **LDP**—maps unicast IP destinations into labels
- **RSVP, CR–LDP**—used for traffic engineering and resource reservation
- **protocol-independent multicast (PIM)**—used for multicast states label mapping
- **BGP**—external labels (VPN)

The Internet Engineering Task Force (IETF) has also defined a new protocol known as the label distribution protocol (LDP) for explicit signaling and management of the label space. Extensions to the base LDP protocol have also been defined to support explicit routing based on QoS and CoS requirements. These extensions are captured in the constraint-based routing (CR)–LDP protocol definition. It is used to map FECs to labels, which, in turn, create LSPs. LDP sessions are established between LDP peers in the MPLS network (not necessarily adjacent)

5.11 LDP (LABEL DISTRIBUTION PROTOCOL)

LDP Protocol has the following functions:

- Neighbor discovery

Discover directly attached Neighbors—pt-to-ptlinks (including Ethernet)

Establish a session

Exchange prefix/FEC and label information

- Extended Neighbor Discovery

  Establish peer relationship with another router thatis not a neighbor

  Exchange FEC and label information

  May be needed to exchange service labels

5.11.1 TDP (Tag Distribution Protocol)

- Tag Distribution Protocol—Cisco proprietary
  - Pre-cursor to LDP
  - Used for Cisco Tag Switching
- TDP and LDP supported on the same device
  - Per neighbor/link basis
  - Per target basis
- LDP is a superset of TDP
- Uses the same label/TAG
- Has different message formats

5.12 OTHER LABEL DISTRIBUTION PROTOCOL – BGP

- Used in the context of MPLS VPNs
- Need multiprotocol extensions to BGP
- Routers need to be BGP peers

The peers exchange the following types of LDP messages:

- **discovery messages**—announce and maintain the presence of an LSR in a network
- **session messages**—establish, maintain, and terminate sessions between LDP peers
- **advertisement messages**—create, change, and delete label mappings for FECs
- **notification messages**—provide advisory information and signal error information

5.13 SETTING UP LABEL-SWITCHED PATHS (LSPS)

MPLS provides the following two options to set up an LSP:

- **hop-by-hop routing**—Each LSR independently selects the next hop for a given FEC. This methodology is similar to that currently used in IP

networks. The LSR uses any available routing protocols, such as OSPF, ATM private network-to-network interface(PNNI), etc.

- **explicit routing**—Explicit routing is similar to source routing. The ingress LSR (i.e., theLSR where the data flow to the network first starts) specifies the list of nodes through which the ER–LSP traverses. The path specified could be non-optimal, as well. Along thepath, the resources may be reserved to ensure QoS to the data traffic. This eases traffic engineering throughout the network, and differentiated services can be provided using flows based on policies or network management methods.

The LSP setup for an FEC is unidirectional in nature. The return traffic must take another LSP.

5.14 MPLS VPNS

5.14.1 What Is A VPN:

- VPN is a set of sites which are allowed tocommunicate with each other
- VPN is defined by a set of administrative policies
  - *Policies determine both connectivity and QoS among sites*
  - Policies established by VPN customers
  - *Policies could be implemented completely by VPNService Providers*
- Using BGP/MPLS VPN mechanisms
- Flexible inter-site connectivity ranging from complete to partial mesh
- Sites may be either within the same or in different organizations(VPN can be either intranet or extranet)
- Site may be in more than one VPN (VPNs may overlap)
- Not all sites have to be connected to the same service provider (VPN can span multiple providers)

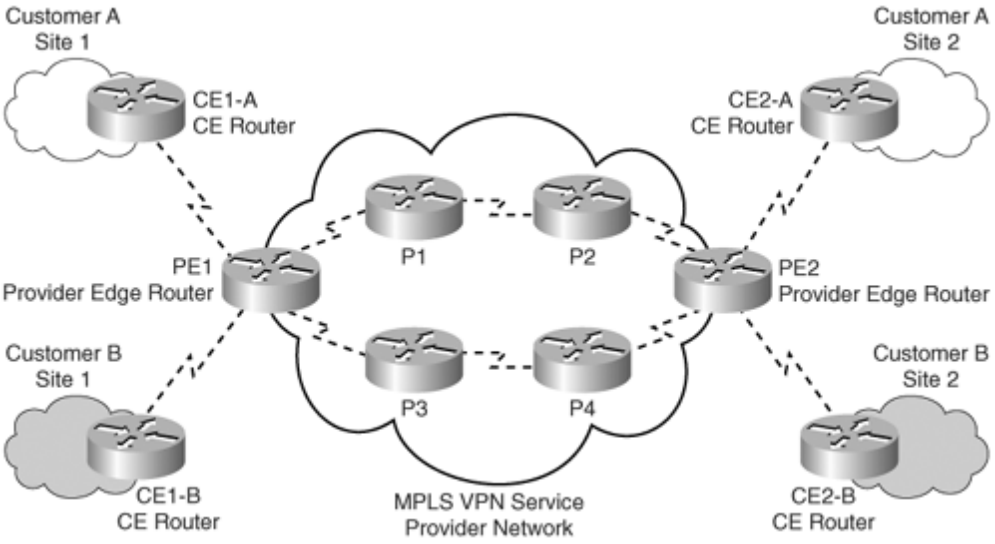


Figure 36: **MPLS VPN Architecture**

Customer network— Consisted of the routers at the various customer sites. The routers connecting individual customers' sites to the service provider network were called customer edge (CE) routers.

Provider network— Used by the service provider to offer dedicated point-to-point links over infrastructure owned by the service provider. Service provider devices to which the CE routers were directly attached were called provider edge (PE) routers. In addition, the service provider network might consist of devices used for forwarding data in the backbone called provider (P) routers.

5.15 CLASSIFICATION OF VPN IMPLEMENTATION

Depending on the service provider's participation in customer routing, the VPN implementations can be classified broadly into one of the following:

- Overlay model
- Peer-to-peer model

5.15.1 Overlay Model

1. Service provider doesn't participate in customers routing, only provides transport to customer data using virtual point-to-point links. As a result, the service provider would only provide customers with virtual circuit connectivity at Layer 2.
2. If the virtual circuit was permanent or available for use by the customer at all times, it was called a permanent virtual circuit (PVC).
3. If the circuit was established by the provider on-demand, it was called a switched virtual circuit (SVC).

4. The primary drawback of an Overlay model was the full mesh of virtual circuits between all customer sites for optimal connectivity. It resembles the physical mesh connectivity in case of leased lines. Overlay VPNs were initially implemented by the SP by providing either Layer 1 (physical layer) connectivity or a Layer 2 transport circuit between customer sites.

   In the Layer 1 implementation, the SP would provide physical layer connectivity between customer sites, and the customer was responsible for all other layers. In the Layer 2 implementation, the SP was responsible for transportation of Layer 2 frames (or cells) between customer sites, which was traditionally implemented using either Frame Relay or ATM switches as PE devices. Therefore, the service provider was not aware of customer routing or routes.

Later, overlay VPNs were also implemented using VPN services over IP (Layer 3) with tunneling protocols like L2TP, GRE, and IPSec to interconnect customer sites. In all cases, the SP network was transparent to the customer, and the routing protocols were run directly between customer routers

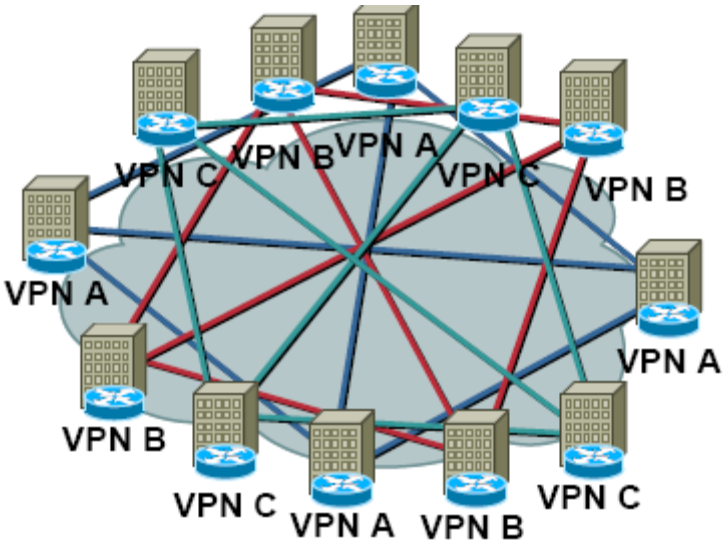


Figure 37: **Overlay VPN**

5.15.2 Peer-To-Peer Model

The peer-to-peer model was developed to overcome the drawbacks of the Overlay model and provide customers with optimal data transport via the SP backbone. Hence, the service provider would actively participate in customer routing. In the peer-to-peer model, routing information is exchanged between the customer routers and the service provider routers, and customer data is transported across the service provider's core, optimally. Customer routing information is carried between routers in the provider network (P and PE routers) and customer network (CE routers). The peer-to-peer model, consequently, does not require the creation of virtual circuits. The CE routers exchange routes with the connected PE routers in the SP domain. Customer routing information is

propagated across the SP backbone between PE and P routers and identifies the optimal path from one customer site to another.

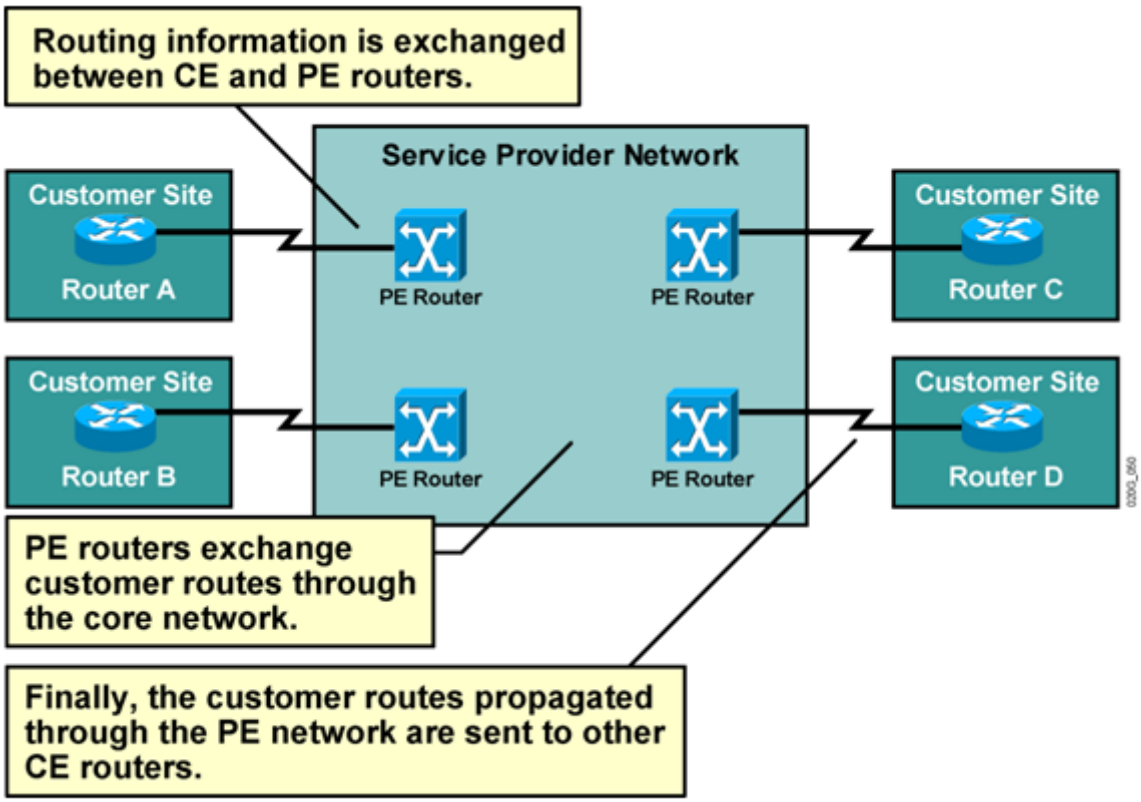


Figure 38: **Peer – to – Peer VPN**

5.16 DIAL VPN SERVICE

Mobile users of a corporate customer need to access their Corporate Network from remote sites. Dial VPN service enables to provide secure remote access to the mobile users of the Corporate. Dial VPN service, eliminates the burden of owning and maintaining remote access servers, modems, and phone lines at the Corporate Customer side.

5.17 LAYER 2 AND LAYER 3 VPNS

- Layer 2 VPNs

  - Customer End points (CPE) connected via layer 2 such as FrameRelay DLCI, ATM VC or point to point connection

  - If it connects IP routers then peering or routing relationship is between the end points

- Multiple logical connections (one with each end point)

➢ Layer 3 VPNs

- Customer end points peer with provider routersSingle peering relationship
- No mesh of connections
- -Provider network responsible for
- Distributing routing information to VPN sites
- Separation of routing tables from one VPN to another

5.18 MPLS VPN WORKING

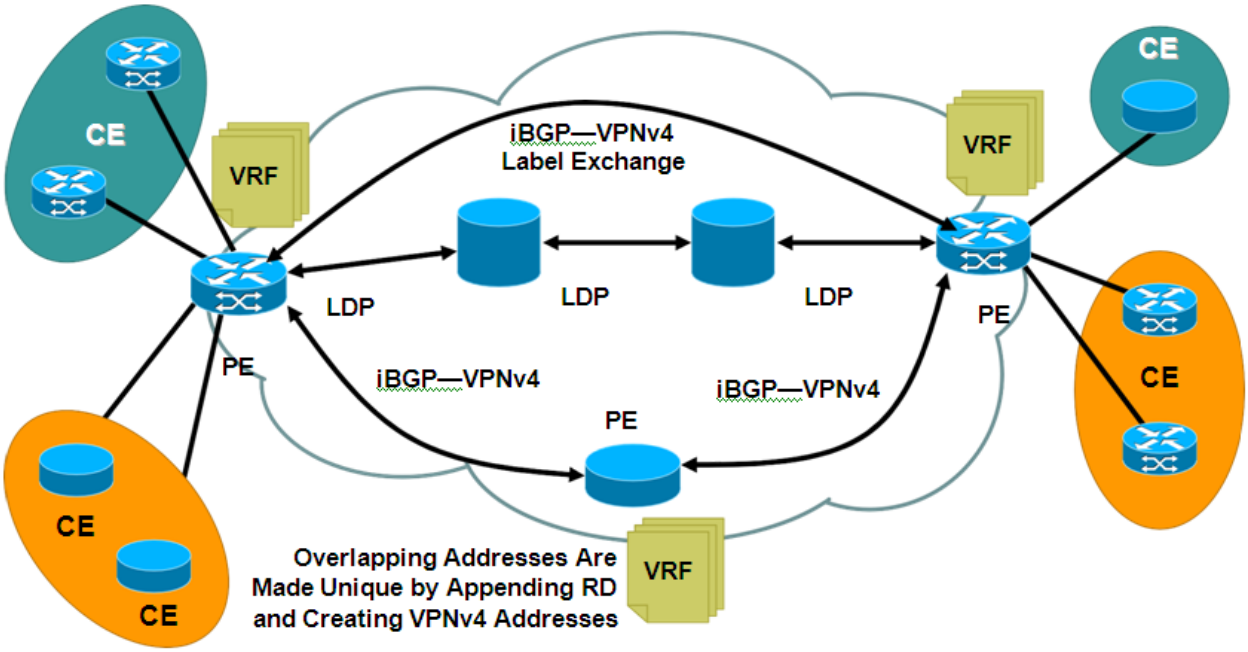


Figure 39: **MPLS VPN working**

5.19 MPLS LER ARCHITECTURE:

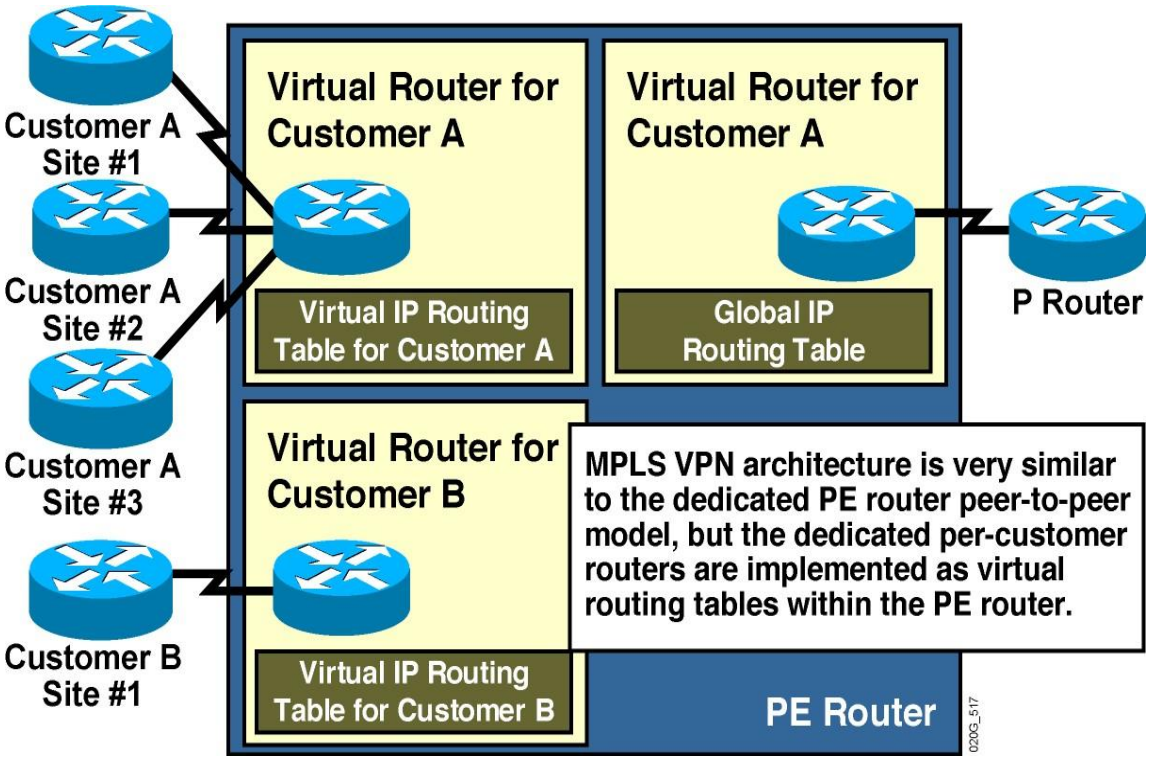
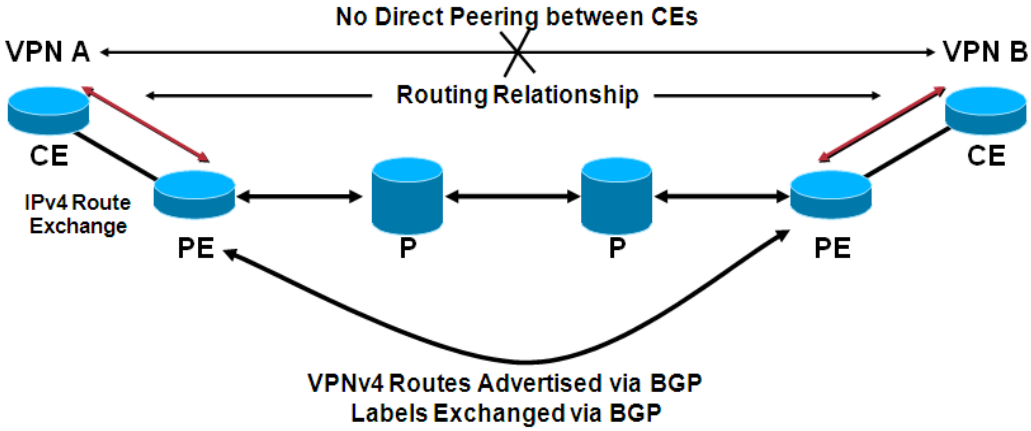


Figure 40: **MPLS LER architecture**

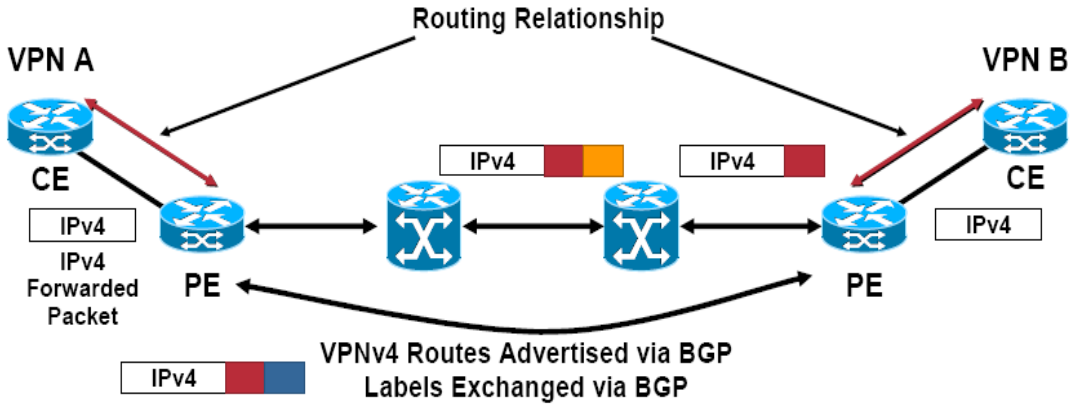
5.19.1 MPLS Control Plane Path:



- RD—8 Byte field—assigned by provider—significant to the provider network only
- VPNv4 Address: RD+VPN Prefix
- Unique RD per VPN makes the VPNv4 address unique

Figure 41: **MPLS control path**

5.19.2 MPLS Data Plane Path:



- Ingress PE is imposing 2 labels

Figure 42: **MPLS data plane path**

5.20 ADVANTAGES OF MPLS VPNS OVER OTHER TECHNOLOGIES

BSNL's primary objectives in setting up the BGP/MPLS VPN network are:

1. Provide a diversified range of services (Layer 2, Layer 3 VPNs) to meet the requirements of the entire spectrum of customers from Small and Medium to Large business enterprises and financial institutions.
2. Make the service very simple for customers to use even if they lack experience in IP routing.
3. Make the service very scalable and flexible to facilitate large-scale deployment.
4. Provide a reliable and amenable service.
5. Offering SLA to customers.
6. Capable of meeting a wide range of customer requirements, including security, quality of Service (QOS) and any-to-any connectivity.
7. Capable of offering fully managed services to customers.
8. Allow BSNL to introduce additional services such as bandwidth on demand etc. over the same network.

5.21 CONCLUSION

MPLS was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients, which provide a data-gram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, Frame relay and Ethernet frames. The IP network has emerged as the network for providing converged, differentiated classed of services to user with optimal use of resources and also to address the issues related to Class of service (CoS) and Quality of Service (QoS). MPLS is the technology that addresses all the issues in the most efficient manner and uses labels to make data forwarding decisions.

6 PSTN NETWORK & SERVICES

6.1 LEARNING OBJECTIVES

- Explain the PSTN Network Organization
- Explain the PSTN Services.
- Explain the IN services.

6.2 INTRODUCTION

Telecommunication industry is changing at a rapid pace. Telephony was invented in 1876 and automatic telephone exchanges were developed in 1895. At that time these exchanges were analogue. Then there were digital exchanges in the network, which worked on circuit switching principle, these were called new technology switches e.g. E10B, C.DOT, EWSD, OCB-283,5ESS, AXE-10, etc. Now, packet switching principle is used in the network which is known as Next Generation Network.

6.2.1 Switching In Telecom Network:

In normal telephone service, basically, a circuit or channel between the calling party and called party is set up (temporarily) and this circuit is kept reserved till the call is completed. Here two speech time slots are involved -one of the calling subscriber and other of the called subscriber. It is called circuit switching.

The data networks, on the other hand use the principle of Packet Switching. In Packet switching the information (speech, data etc) is divided into packets each packet containing piece of information also bears source and destination address. These packets are sent independently through the network with the destination address embedded in them. Each packet may follow different path depending upon the network. At the destination point all these received packets are reassembled.

6.3 PSTN NETWORK:

The telephone network used for fixed line services is also referred as PUBLIC SWITCHED TELEPHONE NETWORK (PSTN). There are different types of the telephone exchanges(switching systems) in PSTN. Earlier there were manual type, Electromechanical type like Strowger and Cross bar. E10B was the first digital electronic exchange to be inducted in the network. But it had certain limitations like:

- The ISDN and CCS7 signalling was not supported.
- The traffic handling capacity and BHCA capacity was low.

- In the RLUs in case of link failure with the main exchange local switching within RLU subscribers was not possible. To avoid these problems new technology switching systems were inducted in our network. Mainly 4 NT switching systems were inducted in BSNL network:
- EWSD Supplied by M/s Siemens, Germany
- OCB-283 Supplied by M/s Alcatel, France
- 5ESS Supplied by M/s Lucent, USA
- AXE-10 Supplied by M/s Ericsson

Some new Salient features of New technology switches were:

- All NT exchanges support ISDN, C#7, V5.2, centrex facility.
- The traffic handling capacity and BHCA capacity are sufficient.
- Standalone RSU : All exchanges have this facility while in case of main link with the exchange is down subs of RSU can call among themselves. In 5ESS in standalone condition metering is done while in case of OCB-283 and EWSD metering is not possible. In case of OCB-283 double remoting is possible.

For rural area in our country where small capacity exchanges were required, CDOT equipment (CDOT 128P, 256P, SBM, MBM etc) was installed. CDOT technology is indigenously developed technology in our country. Initially standalone 128P, 256 P CDOT exchanges were installed but later these small independent exchanges have been converted into AN-RAX (Access Network Rural Automatic Exchange) and they were parented to nearby CDOT SBM/MBM or NT exchange. With this development all remote ANRAXs could be maintained from the SBM/MBM . It improved O& M functions/issues of small exchanges. In the BSNL network about 40% of the total switching capacity is on CDOT technology.

Next Generation Network is the framework where a common transport network based on Internet Protocol for provides all kinds of telecommunication services.

6.4 PSTN NETWORK ORGANIZATION:

In BSNL (Earst while DOT), the whole network is divided into circles (25 circles), each circle is divided into SSA (Secondary Switching Area) as an administrative unit. SSA is also known as LDCA(Long Distance Charging Area) and then further one LDCA is divided into many SDCAs(Short Distance Charging Area). This division of LDCA and SDCA is for charging purposes. Normally an inter SDCA but within same LDCA call is charged on the SDCC distance basis and an inter circle call is charged on LDCC distance basis .The telephone network is also referred as PUBLIC SWITCHED TELEPHONE NETWORK (PSTN) .The offered voice service is referred as PLAIN OLD TELEPHONE SERVICE (POTS).

The PSTN network was organized in a hierarchical manner with Lev-1/Lev2/Tandem/Local Exchanges. The calls from a local exchange is routed to level-I TAX either directly or through Lev-II TAX. From Lev-I TAX it is routed to the destination

exchange either directly or through another Lev-I/Lev-II TAX. For ISD calls ISD Gateway is used.

The next generation networks is based on packet switching which involves voice, data and multimedia such as audio and video. The BSNL has planned a huge network wherein all the traditional voice and data customers migrate from C-DOT TDM towards NGN C-DOT. There are phases of migration from circuit switched PSTN to NGN which are done in phased manner in BSNL. NGN provides new services to the customers such as Multi media video conferencing, Wide Area IP Centric, prepaid solution with all functionalities, Personalized Ring Back Tone (PRBT), Fixed Mobile convergence, etc.

6.5 INTERCONNECTION WITH THE PRIVATE OPERATOR:

Any operator can take license for providing Basic telephone service on circle basis Licenses are issued by DOT. Once an operator gets a license in a particular circle, after installing the necessary equipment it is required to be interconnected with the BSNL network for making the calls into/from BSNL network. For this either the connectivity is taken at local exchange level for local calls and also at Lev-I/Lev-II TAX for long distance calls. It is called POI (Point of Interconnection). POI charges are prescribed by TRAI.

6.6 NUMBERING SCHEME IN BSNL

DOT assigns the initial code for all the operators. BSNL having licenses in all the circle in the whole country except Delhi and Mumbai has been assigned digit ‘2’. The actual number which is dialed by the calling subscriber is prefixed with the SDCA code. At present the SDCA code+ Local no are of 10 digits e.g in Jaipur SDCA the local number is identified as 141 (SDCA Code)+2601602(local Number).Some special services like Directory Enquiry (197)., Fault Booking (198), Railway Enquiry (139) etc are provided by these standard short codes using digit ‘1’.

6.7 SERVICES OFFERED ON LANDLINE

6.7.1 ISDN (Integrated Service Digital Network)

ISDN is a powerful tool worldwide for provisioning of different services like voice, data and image transmission over the telephone line through the telephone network. An ISDN subscriber can establish two simultaneous independent calls (except when the terminal equipment is such that it occupies two 'B' channels for one call itself like in video conferencing etc.) on existing pair of wires of the telephone line (Basic rate ISDN) where as only one call is possible at present on the analog line /telephone connection. The two simultaneous calls in ISDN can be of any type like speech, data, image etc. ISDN also supports a whole new set of additional facilities, called Supplementary Services.

6.7.2 Services Offered By ISDN

- Normal Telephone & Fax (G3) and G4 Fax
- Digital Telephone -with a facility to identify the calling subscriber number and other facilities
- Data Transmission at 64 Kbps with ISDN controller card
- Video Conferencing.

6.7.3 Variety Of Supplementary Services Are Supported By ISDN:

- Calling Line Identification Presentation(CLIP)
- Calling Line Identification Restriction(CLIR)
- Multiple Subscriber Number(MSN)
- Terminal Portability(TP)
- Call Hold(CH)
- Call Waiting(CW)
- User to User Signaling (UUSI)

6.7.4 Types Of Accesses

There are two types of "accesses" (connections) for ISDN. Basic Rate Access(BRA): 2B+D 2 Channels of 64 Kbps for Speech And Data.

- 1 Channel of 16 Kbps for Signalling Primary Rate Access (PRA): 30 B+D 30 Channels of 64 Kbps for speech and data.
- 1 Channel of 64 Kbps for signalling.

6.8 SUPPLEMENTARY SERVICES (PHONE PLUS SERVICES)

6.8.1 Abbreviated Dialing

You may be calling a few people very frequently. It is possible to program these numbers as abbreviated codes of 1 or 2 digits. A maximum of 20 numbers can be programmed for abbreviated dialing. It is ideal for STD/ISD. For registration Dial 110+short code (say15)+destination number(with STD code)
For use Dial 111+short code i.e. 11115

6.8.2 Call Waiting

This facility lets you receive incoming calls even when your telephone is busy. You will get a short duration pip-pip tone when you are busy talking , indicating that another call is waiting for you , provided you have activated this facility. You can talk to any one of the callers keeping the other waiting. Complete secrecy of communication between the two callers is maintained. For activation of the service dial: 118 (wait for the tone). For deactivation of the service dial: 119 (wait for the tone).

6.8.3 Hot Line

You may want to be connected directly to a pre-determined number as soon as you lift the hand set even without dialing. At the same time you may want to have the flexibility to dial any other number of your choice. It is possible to have this facility in the digital exchanges by the delayed hotline feature. The number of your choice can be programmed by the exchange staff at your request. After doing so if you lift the telephone and do not dial within 5 seconds , you will be automatically connected to the programmed number. However if you start dialing with in 5 seconds , you can make an outgoing call as usual.

6.8.4 Call Transfer (Call Forward)

Useful for very mobile persons who may not want to miss incoming calls. Using this facility Calls can be forwarded to another telephone number designated by you. For activation Dial 114 and the number for which the call is to be transferred. For deactivation dial 115 and wait for acceptance tone.

6.8.5 Automatic Wake-Up/Reminder Call Service

When you want to be given a reminder at a specific time, all you have to do is to call the exchange and leave the time you want to be reminded. The facility allows you to initiate a call automatically by the exchange at a fixed time specified by the user of the telephone. Dial 116 followed by the time you wish to be reminded or woken-up say at 06.15am (06.15hrs), you will dial 1160615. Dial 117 (the cancellation code) followed by the time you booked the call.

6.8.6 Number/Call Hunting Service

If you have more than one telephone line, this facility is very helpful for your caller. If the called line is engaged, your caller does not have to disconnect and dial other line(s).
This facility automatically transfers the incoming call to whichever line is free.

6.8.7 Calling Line Identification Presentation (CLIP)

The subscriber has to buy separately the CLIP display device from market. Using this facility you can see the number of the calling party before lifting your telephone. Very useful to trace malicious caller. However, the CLIP instrument shall be procured and installed by the users themselves.

6.8.8 Calling Line Identification (CLI)

Announcement Service Dial 164 and listen to the number of the phone line that you have used to make the call. Very useful when in doubt about your phone number.

6.8.9 Electronic Locking For STD/ISD (Dynamic Locking Facility)

For 100% protection against improper use, you can lock your telephone electronically.
Here, you only know the secret code. You can lock/allow Local, STD or ISD calls in many way viz. all calls allowed, only local calls allowed, only STD & Local calls allowed, all outgoing calls barred etc.

6.8.10 To Register Secret Code

Dial 123 0000 ABCD then wait for the acceptance tone (ABCD is the secret code chosen by the subscriber).

To use:
dial 124 ABCD 1 STD/ISD will be barred
dial 124 ABCD 0 STD and ISD will be opened
dial 124 ABCD 3 STD will be opened, ISD barred
dial 124 ABCD 4 STD/ISD and local will be barred
dial 124 ABCD 2 STD/ISD /Trunk call/95 will be barred.

6.8.11 Call Conferencing

With this service telephonic conference can be set up within 3 or more parties.

6.9 IN SERVICES

The term Intelligent Networks (IN) is used to describe an architectural concept which is intended to be applicable to all telecommunications networks and aims to ease the introduction and management of new services. The objective of IN is to allow the inclusion of additional capabilities to facilitate provisioning of service, independent of the existing network capabilities. There are many new services implementation of which requires substantial changes in the existing switches belonging to different vendors. It not only very time consuming but often uneconomical too. Now, with IN technology it is possible to introduce new services rapidly without affecting the available services.

The IN's main advantage is the ability to control switching and service execution from a small set of Intelligent Network nodes known as Service Control Points (SCP).These SCPs are though very few in numbers (two in BSNL network) but can control thousands of switches.

6.10 WHY IT IS CALLED INTELLIGENT?

An intelligent network (IN) is a service-independent telecommunications network. That is, intelligence is taken out of the switch and placed in computer nodes that i.e. SCP. So to implement a IN service, intelligence of the switch with which the customer (sending the request for an IN service by dialling) is connected, is not used. Switches simply forward the

requests of customers for IN services to concerned IN node i.e. SCP. It is this SCP which uses its intelligence and directs the requesting node to take particular action. Forwarding switches simply obey the orders of their IN nodes.

6.10.1 IN Architecture

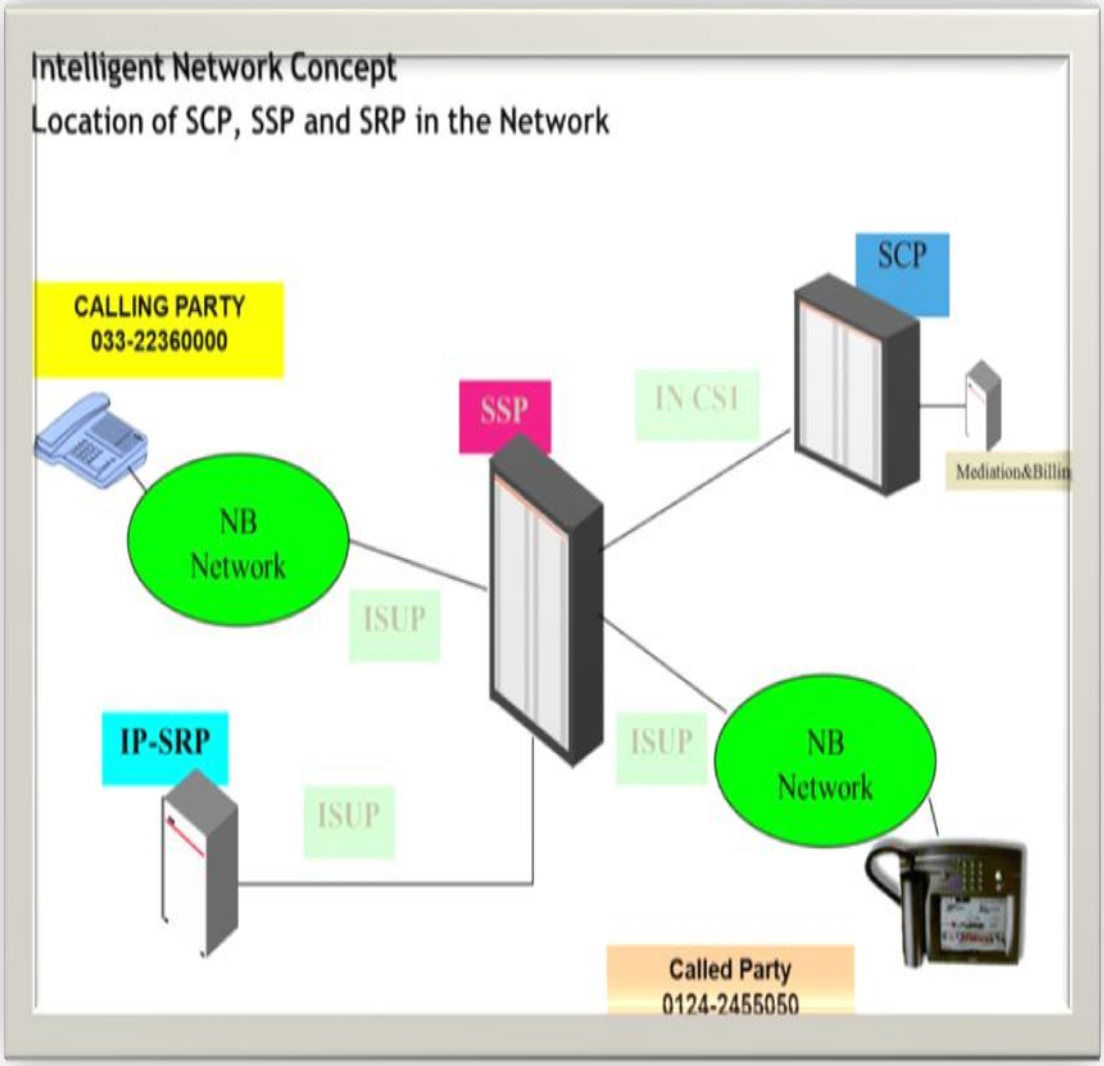


Figure 43: **IN ARCHITECTURE**

6.11 NETWORK ELEMENTS OF IN PLATFORM

1. SSP: Service Switching Point
2. SCP: Service Control Point
3. SMP: Service Management Point
4. IP : Intelligent Peripheral

6.11.1 Service Switching Point (SSP)

The SSP serves as an access point for IN services. All IN service calls must first be routed through the PSTN to the "nearest" SSP. The SSP identifies the incoming call as an IN service call by analysing the initial digits (comprising the "Service Key")dialled by the calling subscriber and launches a Transaction Capabilities Application Part (TCAP) query to the SCP after suspending further call processing. When a TCAP response is obtained from SCP containing advice for further call processing, SSP resumes call processing.
The interface between the SCP and the SSP is G.703 digital trunk. The MTP,SCCP, TCAP and INAP protocols of the CCS7 protocol stack are defined at this interface

6.11.2 Service Control Point (SCP)

The SCP is a fault-tolerant online computer system. It communicates with SSP's and the IP for providing guidelines on handling IN service calls. The physical interface to the SSP's is G.703 digital trunk. It communicates with the IP via the requesting SSP for connecting specialized resources.SCP stores large amounts of data concerning the network, service logic, and the IN customers. For this, secondary storage and I/O devices are supported. The service programs and the data at the SCP are updated from the SMP.

6.11.3 Service Management Point (SMP)

The SMP, which is a computer system, is the front-end to the SCP and provides the user interface. It is sometimes referred to as the Service Management System (SMS). It updates the SCP with new data and programs (service logic) and collects statistics from it. The SMP also enables the service subscriber to control his own service parameters via a remote terminal connected through dial-up connection or X.25 PSPDN. This modification is filtered or validated by the network operator before replicating it on the SCP. The SMP may contain the service creation environment as well. In that case the new services are created and validated first on the SMP before downloading to the SCP. One SMP may be used to manage more than one SCP's.

6.11.4 Intelligent Peripheral (IP)

The IP provides enhanced services to all the SSP's in an IN under the control of the SCP. It is centralized since it is more economical for several users to share the specialized resources available in the IP which may be too expensive to replicate in all the SSPs. The following are examples of resources that may be provided by an IP:

- Voice response system
- Announcements
- Voice mail boxes
- Speech recognition system
- Text-to-speech converters

6.12 IN SERVICES

The various IN services are :

- **Tele-Voting**: Televoting is unique service used in collecting public opinion. A user who wishes to vote, can dial the specific voting number to register his vote of choice. Televoting is possible from STD barred phones also. Televoting is a more cost-effective method of democratic deliberation as it does not require the participants/voter to meet in person. Televoting numbers are 13 digit number :

  1803-424-ABCD-XY (no charge to voter, service subscriber to pay)

  1861-424-ABCD-XY (unit pulse charge to voter)

  1862-424-ABCD-XY (two pulse charge to voter)

- **Voice VPN** : What is true of all VPNs is that they provide connectivity between two or more places using a previously established, shared network infrastructure rather than having to deploy new, dedicated hardware specifically for this purpose. Combined voice VPN can be provided for fixed line telephones of BSNL/MTNL and BSNL mobile. Use this service by dialing short codes to have a private network using public network resources. This service brings down telephone bills due to special package tariff for calls within VPN.
  11 digit number 1801-XYZ-ABCD

- **Toll Free Number** : This service shows the new function in charging, a call to a service subscriber will be paid by the called party. All charges are levied on the service subscriber. The service is free of any charge to the calling user. Service is accessible from networks of other Operators also
  11 digit number 1800-XYZ-ABCD

6.13 CONCLUSION

PSTN services once implemented, they were not easily modified to meet individual customer's requirements. Often, the network operator negotiated the change with the switch vendor. As a result of this process, it took years to plan and implement services. Intelligent network (IN) services are service-independent telecommunications network. That is, intelligence is taken out of the switch and placed in computer nodes that are distributed throughout the network. This provides the network operator with the means to develop and control services more efficiently. New capabilities can be rapidly introduced into the network. Once introduced, services are easily customized to meet individual customer's needs.

7 NGN ARCHITECTURE AND IMPLEMENTATION

7.1 LEARNING OBJECTIVES

- NGN – Vision And Definition
- Protocols Used In NGN
- Migration From PSTN To NGN
- NGN Deployment In BSNL

7.2 INTRODUCTION

Telecommunication industry is changing at a rapid pace. This change in the industry is basically driven by demand of new services from subscriber's side and urge to reduce CAPEX (Capital Expenditure) and OPEX (Operational Expenditure) from carrier side. Today All most all telecommunication giants are installing and maintaining at least three kinds of basic Network.

PSTN: Public Switch Telephone Network was basically developed and engineered for giving voice connectivity to the wire line subscribers. The network consists of Local exchange/RSU as a part of Access Network and TAXs as a part of core Network. Already huge amount of money has been invested in PSTN setup. Because of tough competition from Mobile & Voice over IP, it is becoming white elephant day by day for the operators. Another fact about PSTN is that most of its equipment are going to exhaust their lives in coming years.

PLMN: (Public Land Mobile Network): PLMN has been developed to provide voice services for wireless subscribers. Recent times SMS has emerged as killer application for mobile. PLMN includes BTS/BSC as access network and MSC as a core Network.

Data Network: This network was basically designed for accessing remote files and servers for defense people and universities but now a days nobody can think of living with data network services. The basic and most popular application of data networks is Internet. Other applications include E-commerce, online banking, online gaming, E-shopping, IPTV Video on demand and many more. Data network is an assembly of routers, which are responsible for forwarding information from one end to other.

The interesting fact about the current generation is that these networks have been developed during different time zones. That's why they are separate network infrastructure. There is no sharing of infrastructure among them. However some gateways are available for inter network communication.

Another disadvantage of the current scenario is that all the three networks are having their own service platforms in other words, services are tightly coupled with their networks because carriers or operators have to introduce service separately for separate networks. Because all the three networks are having separate access transport and switching network service providers has to invest in all the three networks separately.

Hence CAPEX increases on the other hand for maintenance of three different networks operational cost also increases. Manpower of the company has to have knowledge of multiple technologies.

7.2.1 NGN Vision

Next Generation Network is the framework where operator will have a common transportnetwork based on Internet Protocol for providing all kinds of telecommunication services. Hence operators will have to install and maintain only a single network which will reduce its CAPEX and OPEX significantly. Moreover service provisioning will become easier because of the introduction of new and intelligent servers. NGN is able to provide Vendor independence because of the standard protocols it uses for interaction withnetwork elements.

7.2.2 NGN Definition

A Next Generation Network (NGN) is a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and services of their choice. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users.

7.2.3 Generalized Mobility:

At present subscribers are enjoying terminal mobility where a network identification system is available in the form of SIM and the same is inserted in the terminal. If user is having that terminal he will be mobile with the identity of the SIM.

In NGN subscriber can have Generalized mobility. Here, each individual will have its own network identity in the form of "SIPURL: xyz @ domain name.com". Users have to make registration from his devices against the given URL. Registrar servers of the company will maintain bindings with URL and physical location of registered devices. Users can register for more than one device at a time. With this subscribers need not to depend upon specific terminal. They can login with any device enabled with required protocols (SIP) and call will come to that device.

7.3 PSTN VERSUS NGN:

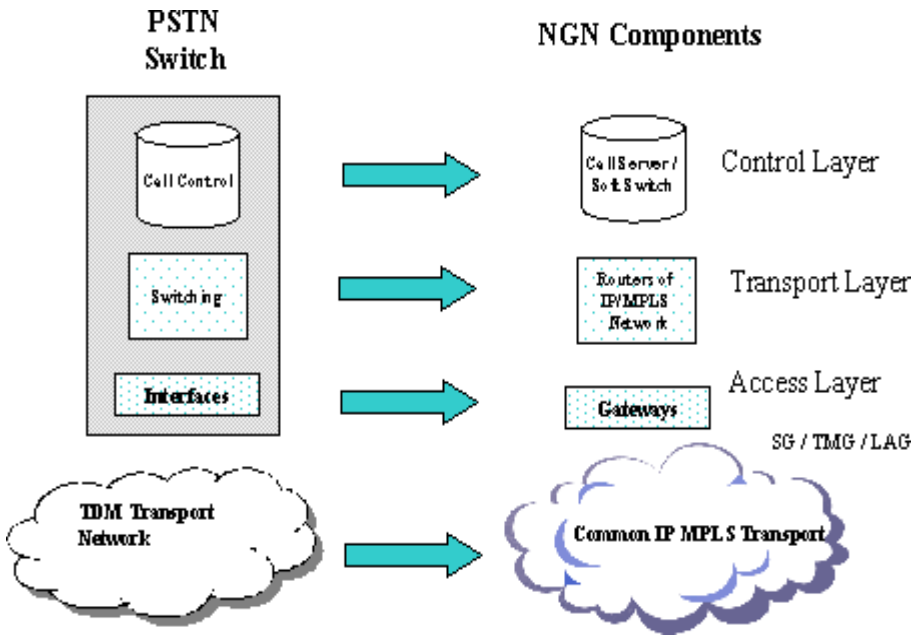


Figure 44: **: PSTN versus NGN**

As shown in above figure PSTN Switch consists of interface, Switching and call control. All the functional entities are shown in one box that means they are interacting with each other using proprietary protocol. Where as in NGN model entities are interacting using standard protocols.

- In PSTN each node should have call control separately whereas NGN may have centralised call control
- PSTN is dedicated network for providing voice services to the subscribers whereas NGN is developing with the idea of carrying all kind of traffic over it.
- PSTN is working on circuit switched principle whereas NGN is working on Packet switching.
- PSTN provides excellent quality of voice and it is tested in all conditions whereas NGN will provide good quality of voice and it is to be tested in adverse network conditions.
- In PSTN service integration is very difficult and because of vendor dependent technologies, it is difficult to introduce services easily. Whereas NGN is able to provide a separate service platform for introduction of services without depending upon underlying network related technologies.

7.4 NGN ARCHITECTURE

NGN is a layered architecture consisting of transport, access, control and application layer. It is important to note that all the layers are independent from each other. Change in one layer should not affect other layers.

7.5 ACCESS LAYER

Access Layers is responsible for direct subscriber attachment function. NGN can support all kind of existing access as well as upcoming access. NGN is capable of processing traffic originated from PSTN, GSM, CDMA, xDSL, WiMAX or any other access system. Depending upon the type of access, protocol conversion and/or media conversionmay be required at the NGN Gateways.

Access Layer consists of Gateways. Example of getaways is Media Gateway, Access gateway. Signalling gateway etc. Media gateway terminates media, coming from PSTN/PLMN in E1 / STM. Here, it is responsible for packetisation of media under the instruction of the control layer. After packetisation of information it throws packets to the transport Network. Access gateway is nearer to subscriber. Subscriber can directly be terminated in Access Gateway. All the required configuration of such subscribers should be done at the control layer. Access Gateway and Media Gateways are responsible for carriage of Media whereas Signalling gateway is carrying signalling generated by PSTN and informs Control Layer about the signalling in required format.

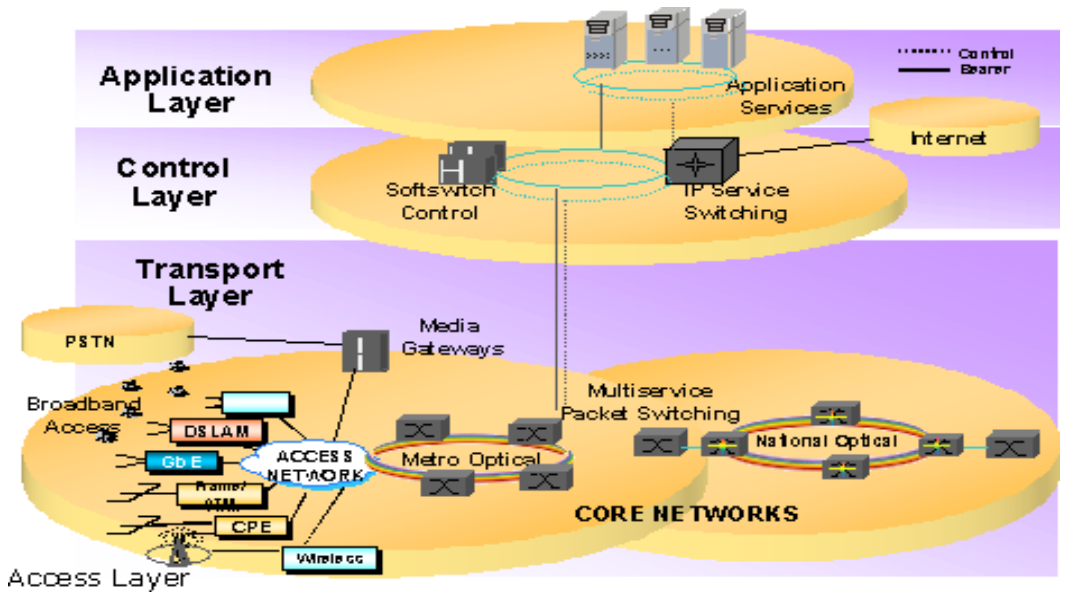


Figure 45: **NGN Architecture**

7.5.1 Transport Layer

Transport Layer of NGN is based on IP (Internet Protocol). It can utilize the advantage ofMPLS (Multi Protocol Label Switching). Transport Layer forms the core of the Network. It basically consists of Routers, which are responsible for carrying traffic originated by access layer. As the same core network is going to be used for all kinds of subscribers enjoying different kind of real time and non real time services, it should be able to make use of band width policies and Qos policies. Operator has to think of managed Network for its subscribers. It is basically an assembly of routers connected with optical network. Traffic coming from gateways is properly routed by those routers.

7.5.2 Control Layer

It is responsible for call setup, routing and charging policies and other controls in NGN environment. It consists of call servers where all information of the network resides. These call servers are responsible for setting up, modifying, charging and tear down ofthe calls. NGN may work on the soft switch principle. It consists of MGC (Media Gateway Controller) as an overall controller and MGs(Media Gateway) for termination of traffic. MGC is basically a server and it is having all the necessary information of network MGC instructs MGs for establishing the call. Under the control of MGC, MG performs different call related tasks such as connection, modification and termination of media streams, packetisation of media etc.

7.5.3 Application Layer

It is responsible for OSS/BSS. Enhanced services to the subscribers will be provided withthe help of application servers. It may include prepaid servers, announcement servers, Service servers etc. Hence NGN is making service separation from Network. Any service can be introduced with the help of server at any time without any modifications in the control, transport or access.

7.6 PROTOCOLS USED IN NGN NETWORK

The main feature of NGN architecture is separation of service, transport and control layers, which are interconnected by open interfaces and use standards protocols.

- **MEGACO** is a protocol which is sponsored from IETF and ITU. It is used inside one MGC (media gateway controller) for controlling media gateways (MG-s). This protocol allows the MGC to tell to the MG-s when to send and receive information towards/from different addresses. This protocol also is useful for sending all information to the MGC from MG-s regarding detected events such is: on –hook, off hook etc. The equivalent protocol of MEGACO according to ITU is H248.

- **SIP**-Session Initiation protocol: is protocol that resides into application layer and is signaling protocol. SIP plays a very important role for session creation for audio/ videoconferences, interactive games and for call orientation towards IP network. SIP is IETF standard which supports traditional telephony services within IP domain such are: routing, identification, call establishment and other services.The job of SIP is limited to only the setup and control of sessions. SIP does not define the structure or content of message body. It is defined by other protocols like SDP(Session Description Protocol). The job of SIP is to carry that description upto destination.

- **SIGTRAN** Between Soft switch and Signalling gateway - sigtran suite of protocols :, shortened form of Signalling Transmission, is the standard for conversion, transport, and encapsulation of SS7 and ISDN over IP. It is one of the most important transition elements in moving from legacy TDM to **NGN** IP

networks.

- **RTP**(Real Time Protocol) Between two media gateways for actual packet transfer-:It is a network protocol for delivering audio and video over IP networks. RTP is used in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications.
- **Real Time Control protocol (RTCP):** is a copy of RTP which offers control services. The main function of RTCP is identification of transport level for one RTP source.

7.7 MIGRATION FROM PSTN TO NGN

Migration from PSTN to NGN should be based on maximum possible reuse of existing equipment and replacement of components which are near the end-of-life.

Migration from PSTN to NGN involves:

- Replacement of TDM network elements in a phased manner
- Maximum reuse of existing resources
- Use of open and mature standards
- Convergence of access and backbone network
- Continuation of existing network capabilities and services with same or comparable QoS and security
- Interworking between different types of networks
- Addition of new services

It is true that NGN can provide operators a better solution for their revenue models. But it is not possible for an incumbent to replace their existing network overnight and install NGN. It will take time to migrate from PSTN to NGN. During that period of time both the networks will coexist. Operators have to follow some strategies to implement NGN in their network. Different phases for migration of PSTN to NGN are given below. However, the sequence of implementation depends on the business and strategic needs of a service provider. Different phases can be combined for implementation.

7.7.1 Phase – I : Migration Of TAX :

In first phase of implementation operators can replace their transit network with softswitch architecture. Operators can make use of the SoftSwitch architecture for the National Long Distance calls.

In PSTN network Local Exchanges (LE) were connected with TAX for Long Distance Calls in turn TAX is connected with PSTN backbone which is carrying the traffic originated by subscribers of Local Exchanges. The setup of TAX and PSTN take care of signaling as well as voice media originated from LE subscribers.

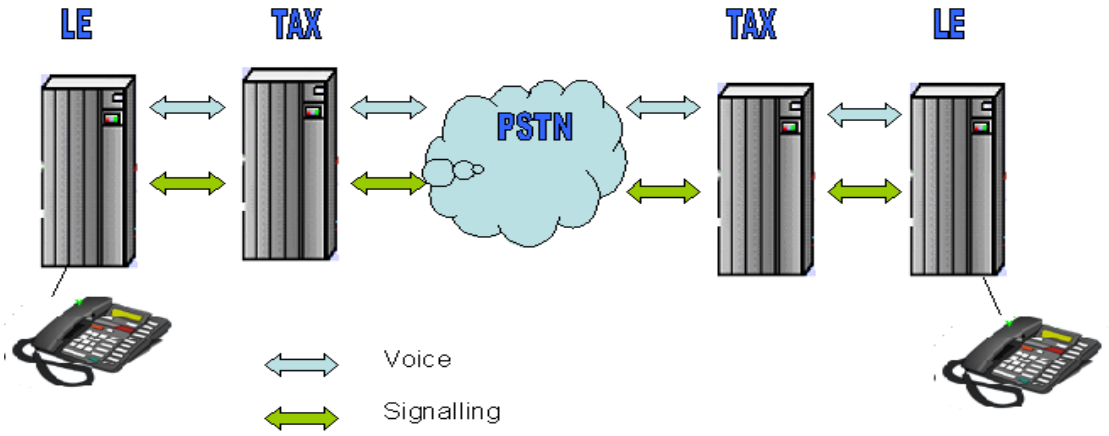


Figure 46: **Phase 1 Migration**

In first phase of migration as discussed TAXs can be replaced by NGN components. **This can be named as IPTAX in general**. For that Local Exchanges have to be connected to Trunk Media Gateways for transportation of Media and will be connected to Signalling Gateway for signaling transport.

Here:

- Normal analog or ISDN subscriber dials the called party number
- PSTN creates CCS#7 Signalling and sends it towards Signalling Gateway.
- Signalling Gateway converts CCS#7 messages to compatible SIGTRAN messages and sends it towards Media Gateway Controller or SoftSwitch.
- After receiving signaling from SG, MGC instruct concerned originating and terminating media gateways to prepare connection for the desired call and at the same time through Signalling Gateway of destination PSTN side MGC / SS inform the destination PSTN exchange about the call. When all the condition for the call is met, MGC instruct concerned originating and terminating media gateways for finally maturing the two communications. Both the MGs convert received TDM voice to packets using Real Time Protocol and vice versa. All the communication between MGC and MG is in H.248 protocol.
- The disconnection of the call is informed by the concerned SG to MGC/SS and thenMGC/SS instructs both the MGs to disconnect the RTP link.

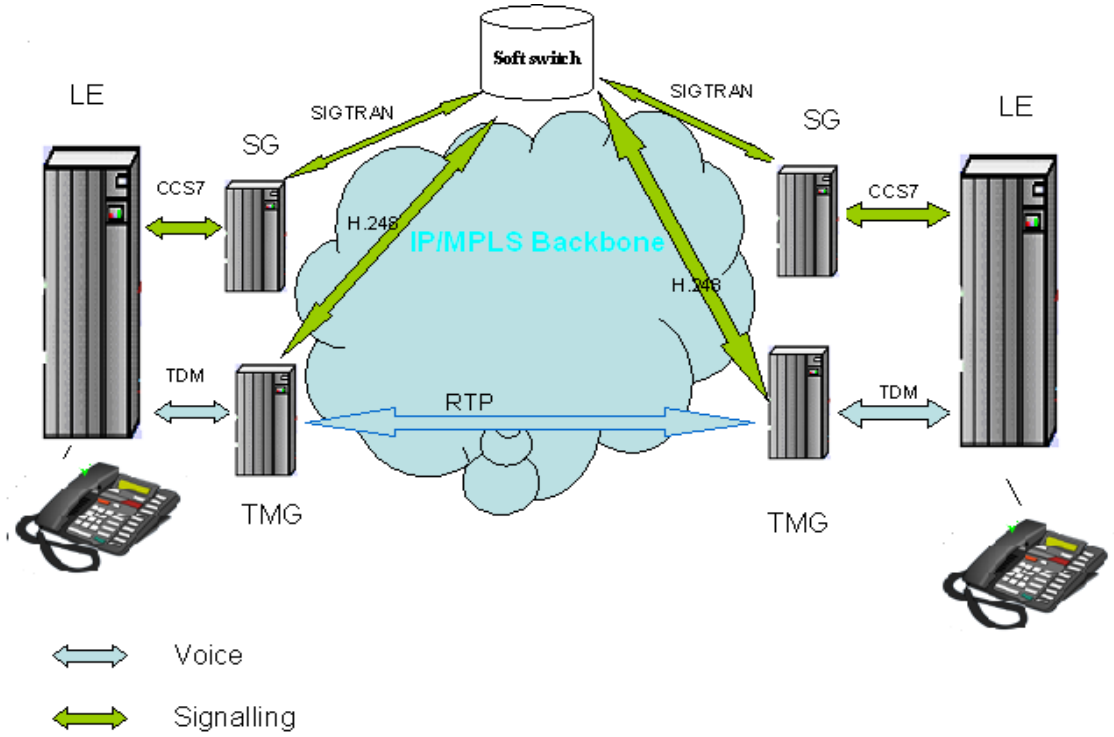


Figure 47: **Phase I-Migration to NGN using TAX replacement**

7.7.2 Phase II: Migration Of Local Exchanges

In this phase Local Exchanges (LEs) are replaced by the Softswitch and Access Gateways (AGW) with the same services. Softswitch with local features will be used as a common control element for class 5 applications. Access Gateways (AG) provide various types of access to the subscribers (e.g. PSTN, ISDN, V5.2, xDSL etc.) and connects them to IP core network. AGWs may be configured for various class 5 applications depending on end user topology, density, service requirements, etc. Depending upon the size of the network, a single softswitch with class 4 and class 5 applications may be planned.

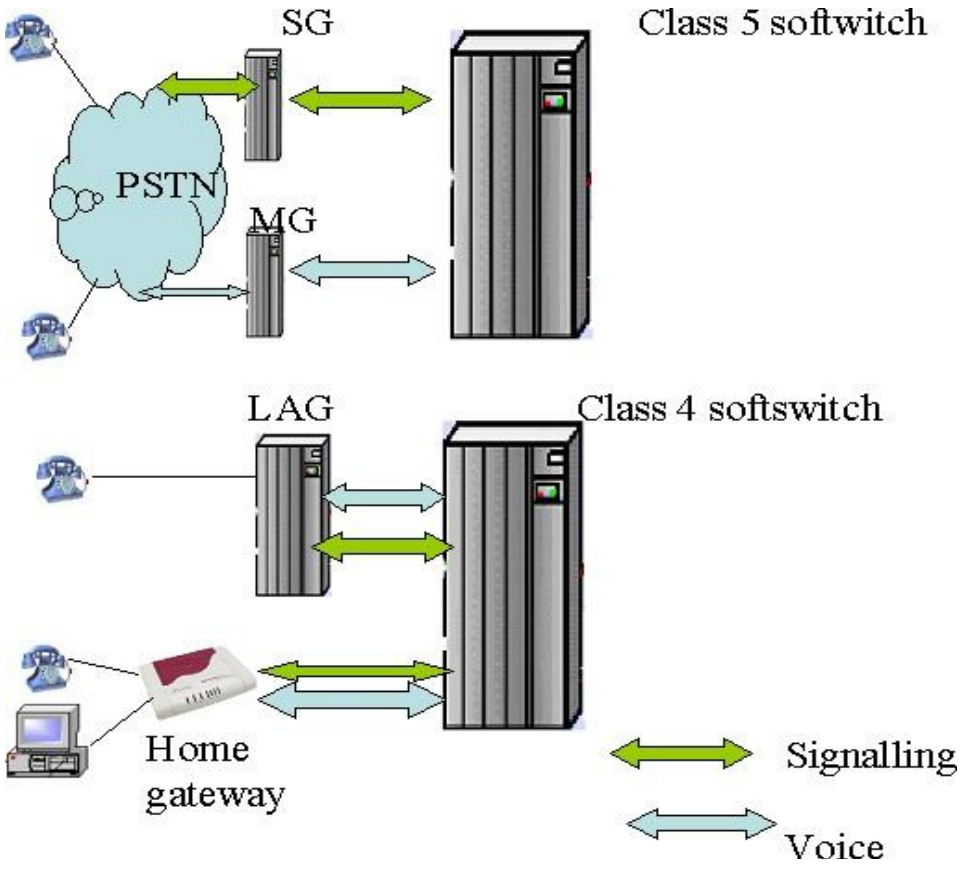


Figure 48: **Phase II: Migration of Local Exchanges**

In soft switch approach there are two types of NGN architecture: (i) Class -4 NGN Architecture (ii) Class -5 NGN Architecture.

The TAX exchanges are called class-4 switches and NGN based TAX is called Class-4 NGN Architecture. Similarly local exchange is called class-5 switch and NGN concept implemented in access network is called Class -5 NGN Architecture.

For migration the operators may first go for Class 4 NGN Architecture and then Class-5 NGN Architecture or some operators may follow a reverse approach. BSNL has adopted the first approach and we have installed Class-4 NGN Architecture i.e. IPTAX.

7.7.3 Phase – III Migration Of Services

While migrating from PSTN to NGN, all PSTN services with the same equipment, same look and feel should be provided. Two PSTN networks connected via NGN transit network should be able to provide transparency to all bearer services. The existing IN services are provided though SCP. The softswitch interacts with SCP through Signalling Gateways, using Intelligent Network Application Protocol (INAP). New IN and value-added services may be implemented using Application Servers (AS) which is accessed by softswitch via Session Initiation Protocol (SIP).

During the migration process new applications may be developed. These new applications along with existing IN services (including prepaid and number portability) are provided by Application Servers.

7.8 NGN DEPLOYMENT IN BSNL NETWORK

The strategy adopted by BSNL would be the overlay one as it has a huge base of circuit switched network that will coexist with packet switched network for a considerable period of time. The migration steps would be as follows :

- Introduce IP in Transit network at Level-1 TAX locations (IP TAX Project) - Class 4 NGN
- Extend IP network to Level-2 TAXs and large scale implementation in Access Network. – Class 5 NGN
- Develop MPLS core at Circle and LDCA Level.
- Offer Voice and Multimedia services to Broadband Subscribers using DSL, Optical Ethernet technologies.

7.9 IP TAX PROJECT : 1ST STEP TOWARDS NGN

The name given to this project has been the IP Tax Project and is a class4 NGN implementation. The equipment for IP Tax is provided by M/s ZTE.

7.9.1 Scope Of IP TAX Project

This project was allocated to ZTE and as per the Solution provided by them, 3 types of sites are built according to different requirements of TMG capacity, and corresponding application scenarios, etc.

- Primary NOC Site
- Primary Site
- Secondary Site

These sites consist of the following products.

- ZTE Soft switch ZXSS10 SS1b,
- Trunk Media Gateways ZXMSG 9000(TMG)
- Announcement Server ZX MSG 9000

7.9.2 Soft Switch Control: ZXSS10 SS1b

The Soft switch control device ZXSS10 SS1b mainly carries out the functions of call control, signaling process, resource management, accounting management, user management and protocol adaptation within its own domain, and uses 100M Ethernet interface to connect to the data network. Soft switch can support maximum load of traffic 2M BHCA/shelf without extension. When extension shelves

(max.8) are present it can support Maximum traffic load of 16M BHCA . Billing records are stored at 3 levels. Maximum capacity of trunk is 200,000 DS0/shelf.

7.9.3 Trunk Media Gateway: ZXMSG 9000

The ZXMSG 9000(Trunk Media Gateway) is located on the core layer of the data MAN for connecting No.7 trunk users and PRI users. It connects the PSTN subscriber to the NGN to implement the conversion between voice/fax on the PSTN/ISDN trunk side and voice/fax on the IP network side. The ZXMSG 9000 can provide the functions of TG, SG and AG through different board and software configurations. When serving as TG, the ZXMSG 9000 is responsible to access PSTN to IP core network through trunk line and convert the voice/fax between PSTN/ISDN trunk side and IP network. It supports 5,600 E1 as Trunk Gateway.

7.9.4 Announcement Server: ZXMSG 9000

ZXMSG 9000 can be configured as announcement server, it is capable to provide sufficient announcement resources for all TMG under its control by interlocking with control device via ZXSS1b.

7.9.5 Network Management: Zxnms

The softswitch integrated network management is developed independently by ZTE, which implement unified network management for softswitch product and relevant devices of ZTE. It can provide centralized management of facilities (Softswitch, TMG, SG, Data devices etc) with unified customer's interface, and can provide management interface for devices of other manufacturers. Every Site connects to MPLS/IP core packet network via a LAN Switch. Different types of sites consisting of the Soft switch control device, the service platform and network management system are constructed that is responsible for the call and service control and network management of the whole network.

7.10 CLASS 5 NGN IMPLEMENTATION:

For Class 5 implementation of Access equipment BSNL has adopted two different approaches:

- Soft Switch based
- IMS based

In Soft Switch based approach BSNL has given tender to M/s CDOT and for IMS based approach tender is given to M/s Huawei with additional capacity tender given to M/s UTSTARCOM.

7.10.1 Softswitch Based Class 5 Implementation.

The scope for the project to be executed by M/s CDOT includes equipment planning for CORE, ACCESS and NOC.

Table 3. Core locations and capacity of CDOT sites

Zone Name	**Primary Softswitch Site**	**DR Softswitch Site**	**Subscriber Ultimate Capacity (Main + DR)**	**NEBS Compliant Chassis/ Server**
North Zone	Gurgaon	Chandigarh	33Lacs + 33Lacs	5 / 48
East Zone	Kolkata	Cuttack	16Lacs + 16Lacs	5 / 48
South Zone	Bangalore	Hyderabad	44Lacs + 44Lacs	5 / 48
West Zone	Pune	Bhopal	29Lacs + 29Lacs	5 / 48

The table above summarizes the CORE locations divided zone wise with capacity of each zone. The zones were divided in Primary site and DR site for redundancy purpose.

7.10.2 IMS Based Approach.

New Technology switches by IMS Class 5 NGN. These Provided by M/s Huawei and M/s UTStarcom. The IMS based project is implemented in two parts consisting of Package-1 IMS core elements and Package-2 Access Elements.

As is done in case of CDOT MAX NGN, IMS is also deployed in core and access parts with core located in four zones.

The Table below summarizes the location of CORE equipments and its capacity.

ZONE	PR Site	DR Site	Subscriber CAPACITY
NORTH	Chandigarh	Lucknow	800000
SOUTH	Hyderabad	Bengaluru	1500000
EAST	Bhubhaneshwar	Kolkatta	500000
WEST	Ahmedabad	Pune	1200000

An additional tender for 2.4 Mn lines is given to M/s UTStarcom, it has deployed core equipment with PR at Chandigarh and DR at Hyderabad site.

Package-2 Access Equipments are supplied by M/s Huawei, M/s ZTE and M/s UTStarcom. The Access equipment called as LMG or Line Media Gateway is a replacement to all the TDM based local exchanges. These LMG's are equipped with both voice and ADSL functionality thus eliminating the use of DSLAM's. The subscriber can avail voice as well as internet services from the same equipment.

7.11 CONCLUSION

Migration to NGN and future networks brings many challenges to network and service providers, telecommunications and media regulators, equipment vendors, and other related business segments, but at the same it provides endless possibilities for rapid innovation of new networks, protocols and services.

8 IP MULTIMEDIA SUBSYSTEM

8.1 LEARNING OBJECTIVES:

- Architecture of IMS
- Different working elements of IMS Core
- IMS interfaces
- Application Servers functionality.

8.2 INTRODUCTION

Many successful services are available today on the Internet, including e-mail, web browsing, chat, and audio and video downloading/streaming, Internet telephony and Multimedia Communications Services. Both fixed and mobile operators face problem of subscriber churn, and the issue is getting worse as new service providers offers cheap, or free, calls over the Internet that continue to arrive on the scene and gain market share. One key way to attract and retain subscribers is to offer differentiation in areas like personalization, service bundling, co-branding, business-to-business relations, tariffs, single sign-on and quality of service.

- Another key way to retain subscribers is to build on and strengthen the customer relationship so that subscribers are far more reluctant to switch suppliers, even if switching means lower call charges in the short term.

In this case, they will have to rapidly push IMS before proprietary solutions become largely adopted. IMS is the only standardized solution in the telecommunications world.

8.3 WHAT IS IMS ?

- IMS – IP Multimedia Subsystem standardized by the telecommunications world is a new architecture based on new concepts, new technologies, new partners and ecosystem.

- IMS provides real-time multimedia sessions (voice session, video session , conference session, etc) and non real-time multimedia sessions (Push to talk, Presence, instant messaging) over an all-IP network.

- IMS targets convergence of services supplied indifferently by different types of networks : fixed, mobile, Internet. IMS is also called Multimedia NGN (Next Generation Network).

- IMS deployment is a strategic decision, not a network technology decision. It can be taken either by a traditional service provider in the context of repositioning its

business on IP services or by any entity that would decide to start an activity in IP services even without owning an access or transport network.

- IMS offers standardized service enablers and network interfaces that will make interoperability of new MM services easier to achieve.
- IMS is a tool for operators that enable the creation and delivery of PS based person-to-person MM services in a way that protects the operator business model and generates new revenue.
- Service scalability is solved by the IMS architecture. It offers support to compose services and expand existing services.
- The core of IMS is combining the best of two worlds datacom industry & telecom industry.

8.4 WHY IMS?

Operator perspective	End-user perspective	General
Quality Of Service	New, exciting services and enhancements of existing services	Faster time to market with new services
Service Integration	Same services available regardless of terminal and access type	Grow and protect subscriber base, increase ARPU
Keeps charging relation with user	Ease of use & Security	Controlling CAPEX and OPEX

Table 4. Operator and End user Perspective

8.5 IMS STANDARDIZATION

The IMS was initially standardized by the 3rd Generation Partnership Projects (3GPP) as part of its Release 5 specifications & is practically speaking targeted at supporting non – real time services .The second release is 3GPP Release 6 & is targeted at supporting real time services .3GPP release added inter-working with WLAN.

With the increasing penetration of Wireless Local Area Networks (WLANs) and emerging Wireless Metropolitan Area Networks (WiMax) as access network technologies, the IMS scope is now extended within the ongoing Release 7 standardization for any IP access network, including fixed access networks, i.e. DSL.

8.6 IMS ARCHITECTURE AS DEFINED BY 3 GPP

The IMS provides all the network entities and procedures to support real-time voice and multimedia IP applications. It uses SIP to support signaling and session control for real-time services. Fig. 1 illustrates the IMS functional architecture. The main functional entity in an IMS is the Call State Control Function (CSCF). A CSCF is a SIP server. Depending on the specific tasks performed by a CSCF, CSCFs can be divided into three different types.

- Serving CSCF (S-CSCF).
- Proxy CSCF (P-CSCF).
- Interrogating CSCF (I-CSCF).

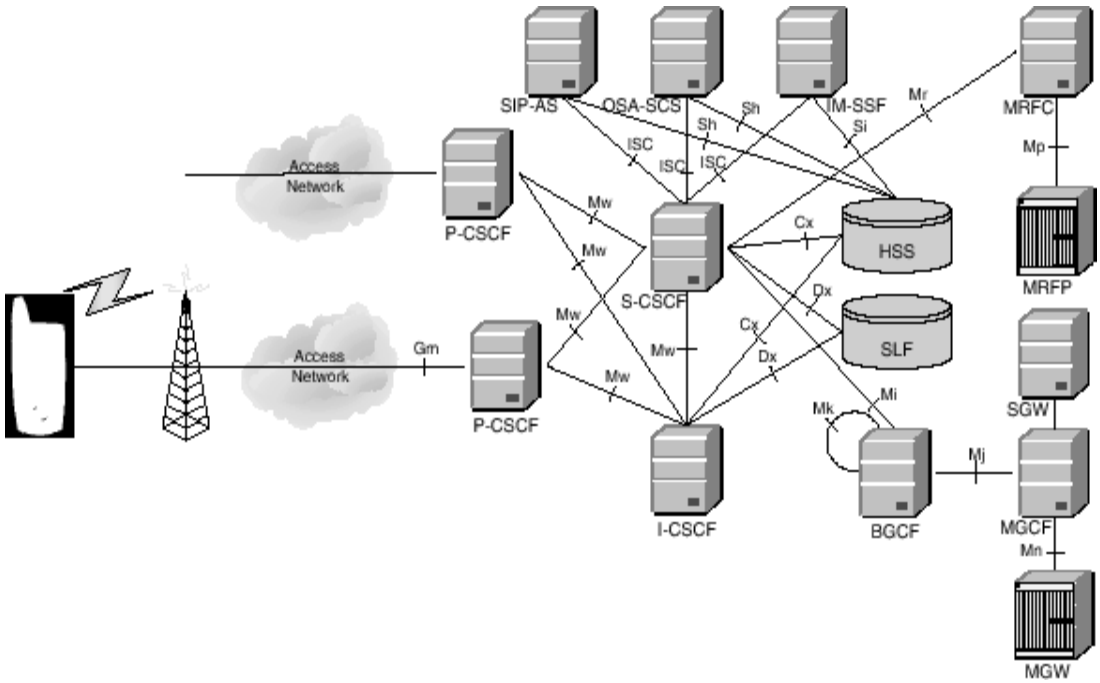


Figure 49:**3GPP IP multimedia subsystems**

8.6.1 S-CSCF (Serving Call State Control Function)

An S-CSCF provides session control services for a user. It maintains session states for a registered user's on-going sessions and performs the following main tasks.

- Registration: An S-CSCF can act as a SIP Registrar to accept users' SIP registration requests and make users' registration and location information available to location servers such as the HSS (Home Subscriber Server).
- Session Control: An S-CSCF can perform SIP session control functionsfor a registered user. Relay SIP requests and responses between callingand called

parties.

- Proxy Server: An S-CSCF may act as a SIP Proxy Server that relays SIP messages between users and other CSCFs or SIP servers.

- Interactions with Application Servers: An S-CSCF acts as the interface to application servers and other IP or legacy service platforms.
- Other functions: An S-CSCF performs a range of other functions not mentioned above. For example, it provides service-related event notifications to users and generates Call Detail Records (CDRs) neededfor accounting and billing

8.6.2 P-CSCF

A P-CSCF is a mobile's first contact point inside a local (or visited) IMS. It acts as a SIP Proxy Server. In other words, the P-CSCF accepts SIP requests from the mobilesand then either serves these requests internally or forwards them to other servers. The P-CSCF includes a Policy Control Function (PCF) that controls the policy regarding

how bearers in the packet-switched network should be used. The P-CSCF performs the following specific functions:

- Forward SIP REGISTER request from a mobile to the mobile's home network. If an I-CSCF is used in the mobile's home network, the P-CSCF will forward the SIP REGISTER request to the I-CSCF. Otherwise, the P-CSCF will forward the SIP REGISTER request to an S-CSCF in the mobile's home network. The P-CSCF determines where a SIP REGISTER request should be forwarded based on the home domain name in the SIP REGISTER Request received from the mobile.
- Forward other SIP messages from a mobile to a SIP server (e.g. themobile's S-CSCF in the mobile's home network). The P-CSCF determines to which SIP server the messages should be forwarded based on the result of the SIP registration process.
- Forward SIP messages from the network to a mobile.
- Compression and decompression of SIP messages. Compression isrequired to minimize the air-interface time.
- Perform necessary modifications to the SIP requests before forwardingthem to other network entities.
- Maintain a security association with the mobile.
- Detect emergency session.
- Create CDRs.

8.6.3 I-CSCF

An I-CSCF is an optional function that can be used to hide an operator networks internal structure from an external network when an I-CSCF is used. It serves as acentral contact point within an operator's network for all sessions destined to a subscriber of that network or a roaming user currently visiting that network. Its main function is to select an S-CSCF

for a user's session, route SIP requests to theselected S-CSCF. The I-CSCF selects an S-CSCF based primarily on the following information:

- Capabilities required by the user.
- Capabilities and availability of the S-CSCF and
- Topological information, such as the location of an S-CSCF and the location of the users P-CSCFs if they are in the same operators network as the S-CSCF.

8.6.4 The Databases: (HSS And SLF)

HSS (Home Subs Server):

- It is just like HLR & Authentication Centre (AuC).
- All the database of users are stored in HSS ie, authentication data , service profile ,charging etc will be in HSS.
- No VLR concept in IMS.
- HSS is mandatory. Whereas SLF is optional.
- HSS is master user database that supports IMS N/W entities that actually handle call.
- It contain subscriber profile , perform authentication & authorisation of the user & can provide information about subscriber location & IP information.

8.6.5 SLF (Subs Location Function)

•Whenever n/w size is so big that if one HSS cannot store data then SLF is required ,this is an addl. Component.

•Suppose S-CSCF has done some authorization then it has to contact HSS for downloading, authentication etc.

–If one HSS is there then no ambiguity.

–But if more than one HSS then SLF will check which HSS.

•Both HSS & SLF communicate through Diameter protocol.

•This diameter is called as AAA protocol.

•SLF will have -(User-ID/ HSS-ID).

Both the HSS and the SLF implement the Diameter protocol (RFC 3588) with an IMS-specific Diameter application.

The Media Gateway Control Function (MGCF) and the IM Media Gateway(IM-MGW) are responsible for signaling and media inter-working, respectively, between the PS domain and circuit-switched networks (e.g. PSTN).

8.6.6 Multimedia Resource Function Processor (MRFP) – Provides Resources To Be Controlled By The MRFC

•Sources media streams (for multimedia announcements)

•Processes media streams (e.g. audio transcoding, media analysis)

•Tones and announcements –Applied on receipt of ACK, self-timed with BYE or stopped on BYE

•Support DTMF within the bearer path.

8.6.7 The Multimedia Resource Function Controller (MRFC)

The Multimedia Resource Function Controller (MRFC) interprets signaling information from an S-CSCF or a SIP-based Application Server and controls the media streams resources in the MRFP accordingly.

8.6.8 The Breakout Gateway Control Function (BGCF)

The Breakout Gateway Control Function (BGCF) selects to which PSTN network a session should be forwarded. IT will then be responsible for forwarding the session signaling to the appropriate MGCF and BGCF in the destination PSTN network.

8.7 REFERENCE INTERFACES:

The main interface in the IMS can be grouped into the following categories:-

Interface for SIP-based signaling and service control:

These include interfaces M_g, M_i, M_j, M_k, M_r, and M_w, which all use SIP as the signalingprotocol.

- Interface M_g allows CSCF to interact with MGCF.
- Interface M_i allows a CSCF to forward session signaling to a BGCF sothat the session can be forwarded to PSTN networks.
- Interface M_j allows a BGCF to forward a session signaling to a selected MGCF that will carry the session to the PSTN.
- Interface M_k allows a BGCF to forward session signaling to another BGCF.
- Interface M_r allows an S-CSCF to interact with an MRFC.
- Interface M_w allows an I-CSCF to direct mobile- terminated session toan S-CSCF.
- Interface for controlling media gateways: These include interfaces M_c & M_p,
- Interface M_c allows a signaling gateway to control media gateway. For example, it is used between an MGCF and an IM-MGW, between an MSC

Server and a CS-MGW, or between a GMSC Server and a CS- MGW.

- Interface M_p, allows an MRFC to control media stream resources provided by an MRFP. Signaling over interfaces M_c and M_p uses the
- H.248 /MegaCo Protocol.

Interfaces with the Information Servers: Interfaces C_x between the CSCF and the HSS allows the CSCF to retrieve from the HSS mobility and routing information regarding a mobile user so that the CSCF can determine how to process a user's sessions. Signaling over C_x interface uses the Diameter Protocol.

Interface with external networks: These include interfaces M_b, M_m, and C_o.

- ✓ Interface M_b, is the standard IP routing and transport interface with external IP networks. The interface M_b may be identical to the G_i interface.
- ✓ Interface M_m is a standard IP-based signaling interface that handles signaling inter-working between the IMS and external IP networks.
- ✓ Interface G_o allows a PCF to apply policy control over the bearer usage in the PS domain.

8.8 SERVICE ARCHITECTURE

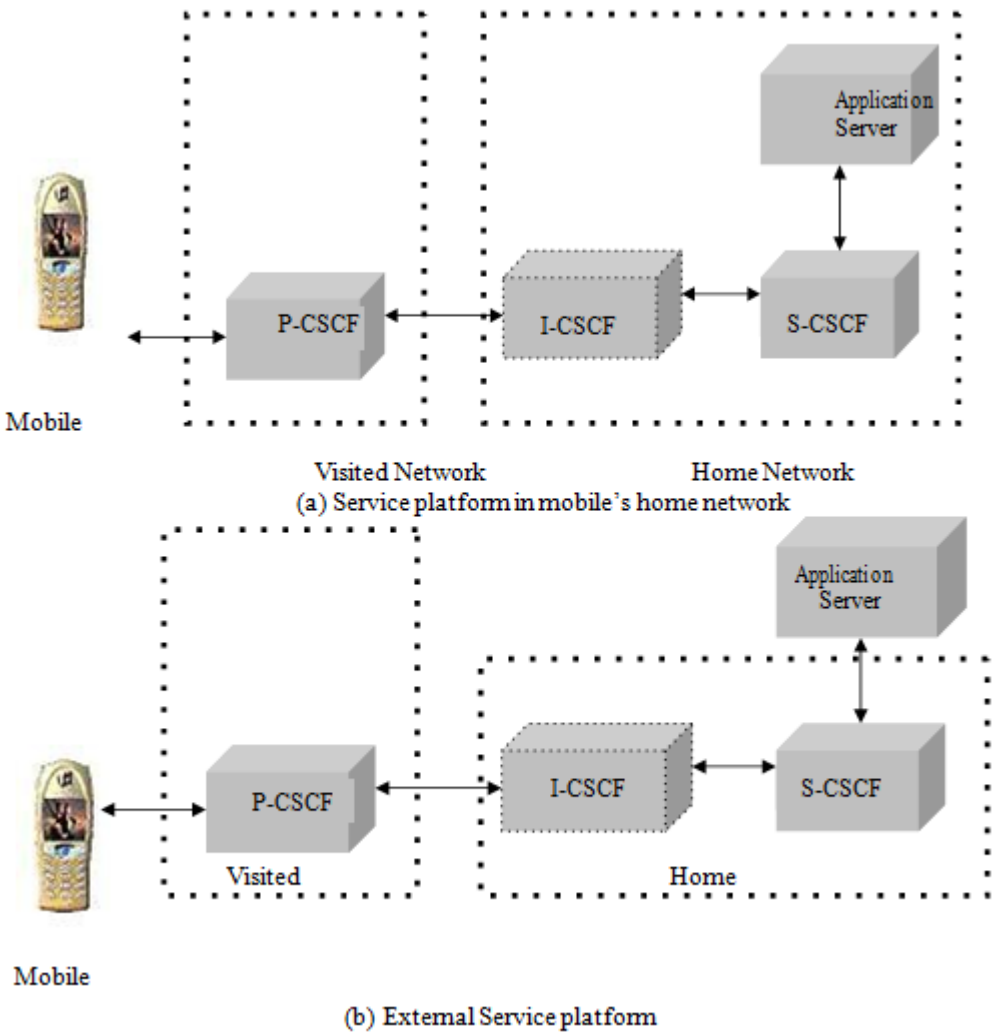


Figure 50: **3GPP Service Architecture**

With both service architectures, the initial SIP request from a mobile travels from the originating mobile to the visited P-CSCF first, which then forwards the request to the I-CSCF (if used) in the originating mobiles home network. This I-CSCF selects an S-CSCF in the home network for this user session and forwards the SIP request to session will travel directly between the visited P-CSCF and the S-CSCF in the mobiles home network.

The S-CSCF is responsible for interfacing with internal and external service platforms as illustrated in Fig. 3. There are three types of standardized platforms:

(1) SIP application server
(2) Open Service Access (OSA) Service Capability Server (SCS) and
(3) IP Multimedia Service Switching Function (IM-SSF).

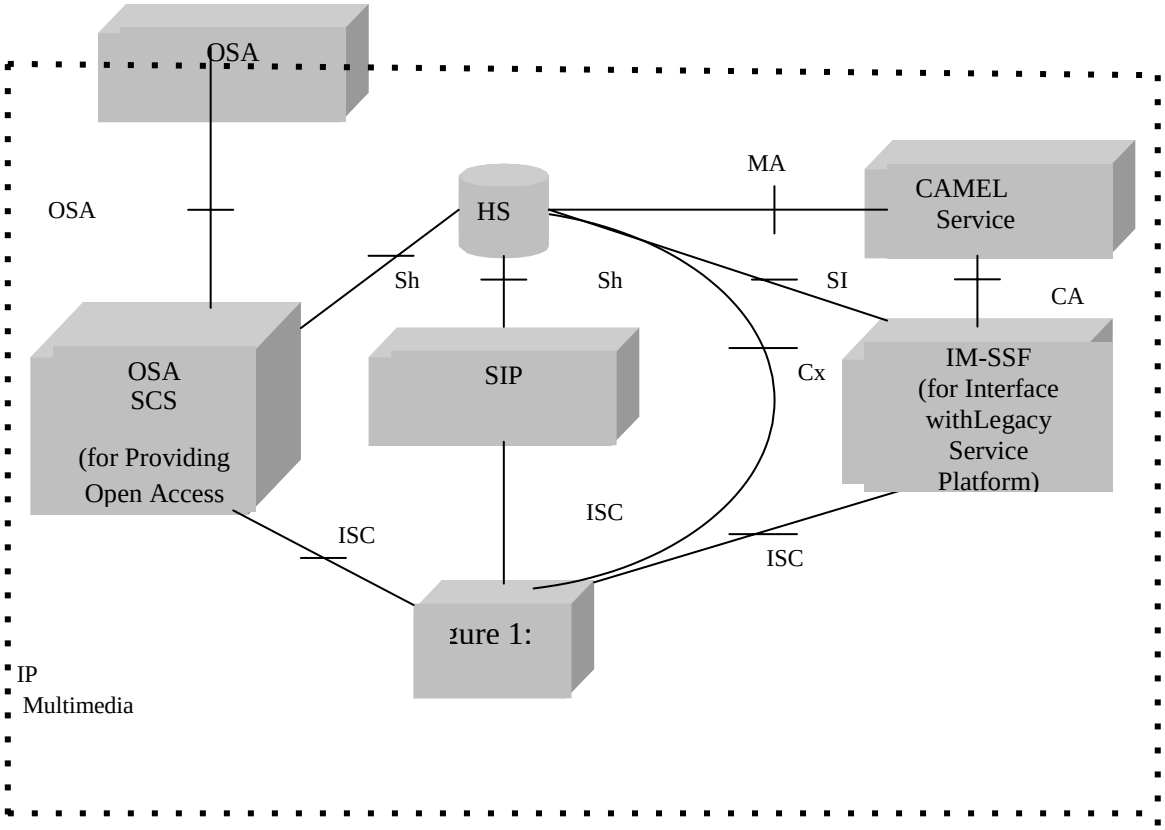


Figure 51: **Interactions between S-CSCF and service platforms**

The services offered by them are value-added services (VAS or operator-specific services. The S-CSCF uses the same interface, IMS Service Control (ISC) interface, to interface with all service platforms. The signaling protocol over the ISC interface is SIP. The OSA SCS and IM-SSF by themselves are not application servers. Instead, they are gateways to other service environments. As depicted in Fig. 3, the OSA SCS and IM-SSF interface to the OSA application server and CAMEL Service Environment (CSE),respectively. From the perspective of the S-CSCF, however, they all exhibit the same ISC interface behavior. The services are briefly described:

8.8.1 SIP Application Server:

In addition to session control, a SIP server can also provide various value-added services. A lightweight SIP-based server enables the CSCF to utilize the SIP-based services and interact with the ISP application servers without additional components.

8.8.2 Camel Service Environment (CSE):

The CSE provides legacy Intelligent Network (IN) services. It allows operators leverage existing infrastructure for IMS services. As specified earlier, the CSCF interacts

with CSE through IM-SSF. The IM-SSF hosts the CAMEL features and interfaces with CSE by CAP (CAMEL Application Part).

8.8.3 OSA Application Server:

Applications may be developed by a third party that is not the owner of the network infrastructure. The OSA application server framework provides a standardized way for a third party to secure access to the IMS. The OSA reference architecture defines an OSA Application Server as the service execution environment for third-party applications. The OSA application server then interfaces with the CSCF through the OSA SCS by OSA API (Application Programming Interface).

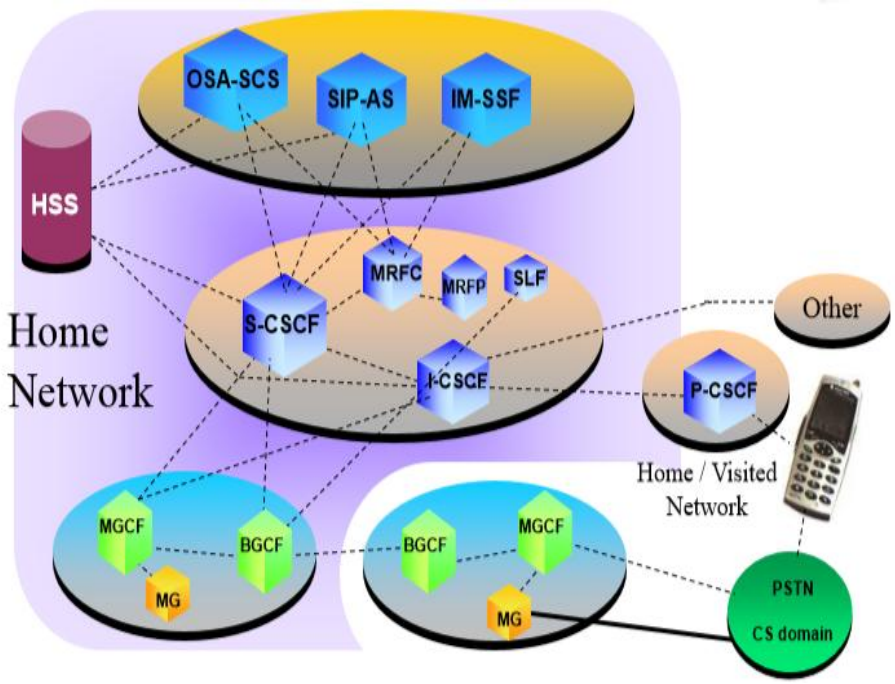


Figure 52: **Simplified 3GPP IMS Architecture**

8.9 CONCLUSION

The IP Multimedia Subsystem (IMS) seems to be the technology that will prevail in Next Generation Networks (NGNs) and its main goal to make convergence between any IP networks and a vertical handoff may happening depend on the user requirements (services, QoS..etc). In this chapter it was presented an IMS based interworking architecture for NGN networking through which it prevail that how any two user from any two different IP based network can be involved in a session under the umbrella of IMS management. By presenting a complete signaling flow for concerning the authorization, registration, session set up and vertical handoff processes between two networks.

9 STAND-ALONE SIGNALING TRANSFER POINT

9.1 LEARNING OBJECTIVES

- Different nodes in signaling networks
- Role of SSTP
- Functions of SSTP
- SSTP deployment in BSNL

9.2 INTRODUCTION

Signaling System No. 7 (SS7) is a signaling protocol that has become a worldwide standard for modern telecommunications networks. SS7 is a layered protocol following the OSI reference model .It enables network elements to share more than just basic call-control information through the many services provided by the SS7's Integrated Services Digital Network-User Part (ISUP), and the Transaction Capabilities Application Part (TCAP). The functions of the TCAP and ISUP layers correspond to the Application Layer of the OSI reference model, and allow for new services such as User-to-User signaling, Closed-User Group, Calling Line Identification, various options on Call Forwarding and the rendering of services based on a centralized database (e.g., 800 and 900 service). All of these services may be offered between any two network subscribers.

9.3 CCS NETWORK ARCHITECTURE

The CCS Network is comprised of Four Major Components:

- Service Switching Points [SSP]
- Signaling Transfer Points [STP]
- Service Control Points [SCP]
- Data Signaling Links (SLK)

An SS7 Network consists of a flat non-hierarchical configuration enabling peer-to-peer Communication. Figure 1: SS7 Common Channel Signaling Networks depicts the makeup and connectivity of SS7 Common Channel Signaling networks.

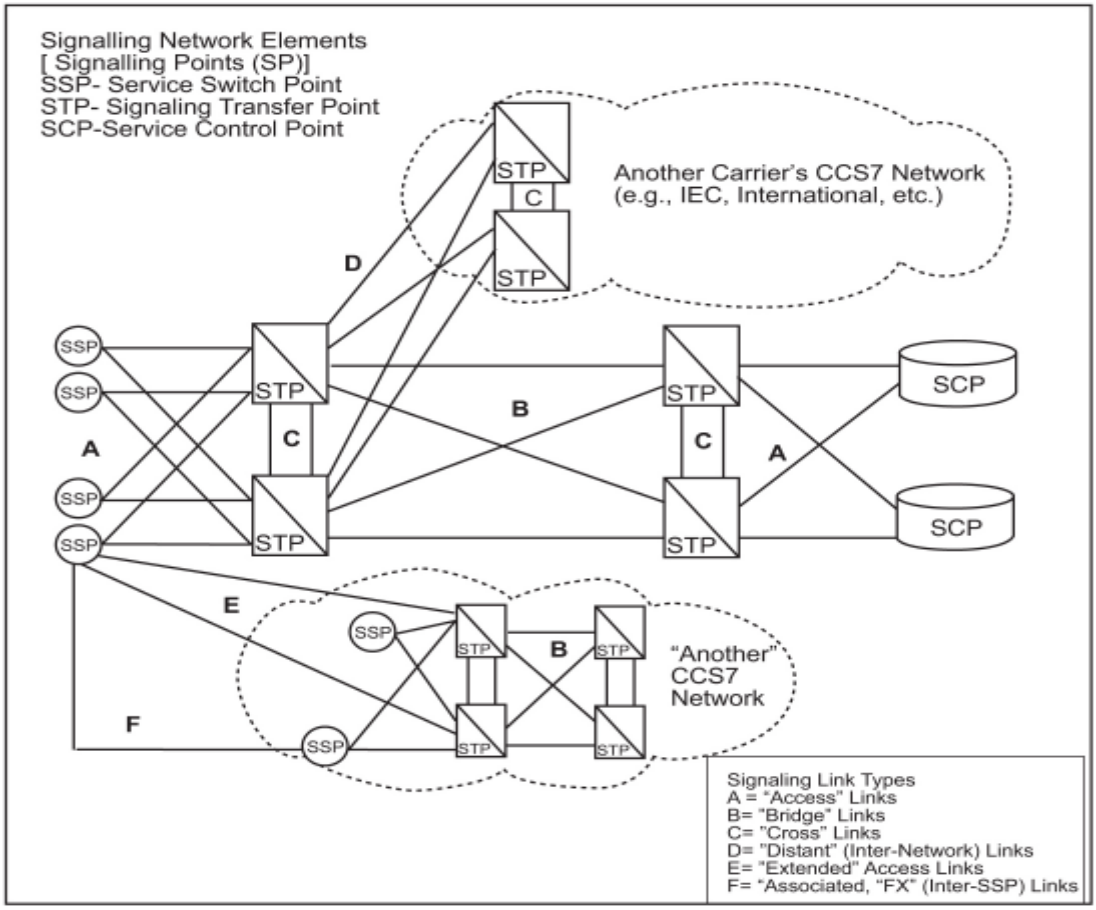


Figure 53: **Common channel signaling networks**

SS7 Common Channel Signaling Networks shows the three principal network elements of SS7 Common Channel Signaling networks, interconnected by the six standard types of signaling links currently in use. Signaling links are data transmission links that ordinarily operate on digital carrier facilities at 64,000 bits per second in most regions of the world. High Speed Links (HSLs) at 2.048 Mbps are used.

Signaling links between any two signaling network elements are deployed in groups called "link sets," dimensioned to carry the estimated signaling traffic between two STPs. Because STPs are deployed in pairs, as shown in Figure, SS7 Common Channel Signaling Networks, an alternate route always exists between any two STPs. One combination of the link sets interconnecting an SSP or SCP with both members of the STP pair is called a "combined link set." The traffic carried between any two signaling network elements is load-shared across links in a link set, rotating through all links available according to the rules of the SS7 protocol.

Traffic destined for any network element through the STP pair is further load-shared over the combined link set, unless restricted by network management rules also established by the SS7 protocol

9.3.1 Service Switching Point (SSP)

The SSPs are the legacy switches of the telecommunications network. SSPs are referred to as an "*End Office switch*", "*Central Office switch*", "Toll Tandem switch", etc. The central offices that house the SSP are identified by classes ranging from a class 5-lowest, to a class 1 – highest office. The lowest class office in a network will be the one providing dial tone to subscribers. SSP is typically found in tandem or Class 5 offices and is the interface to the networks outside of SS7.

A SSP can be any of the following:

- Customer switch
- End office
- Access tandem
- Tandem

Usually, a switch is used to interface to the customer premise, The CO switch then interfaces to the SS7 network via the SSP. The SSP is the interface between the subscriber and the telecom network, and provide the following functions:

9.3.2 Call Processing Function

- Provides dial tone
- Routes calls between links and trunks
- Provides tones, and announcements
- Maintenance and revenue collection and generation

9.3.3 Query Processing

When necessary, it generates queries toward another signaling node or database to receive information necessary for certain calls.

SS7 Response Processing

Upon receiving queried information, carries out the connection function for proper handling of calls.

9.3.4 Resource Interface

For AIN services, establishes and maintains connections to Intelligent Peripherals (IPs)

9.3.5 Service Control Point (SCP)

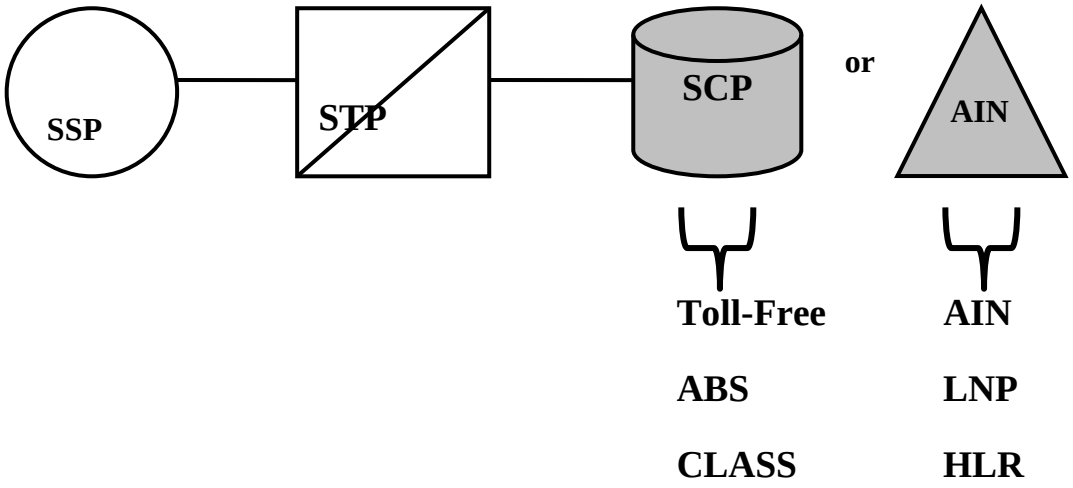


Figure 54: **SCP Connectivity**

The SCPs and AIN SCPs are centralized database that provide real-time access to call completion and information services such as:

- Toll-Free Database Service
- Alternate Billing Service (ABS)
- Custom Local Area Signaling Services (CLASS)
- Advanced Intelligent Network Services (AIN)
- Local Number Portability (LNP)
- Home Location Register (HLR)
- Visitor Location Register (VLR)

9.2.3 Signaling Transfer Point (STP)

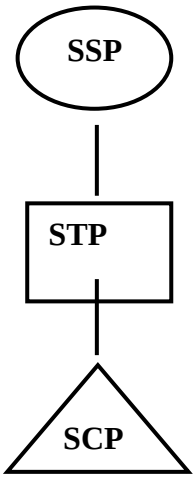


Figure 55: **STP**

STPs are routers that are placed within the heart of the CCS Networks. STPs are packet switches that provide common channel message routing and transport. STPs are stored programmed control switches that use information contained in messages in conjunction with information stored in memory to route messages to the appropriate destination signaling point.

STPs are generally deployed in pairs with mirrored databases. If one of the STPs are removed from service or signaling links fail, the mate can process all of the traffic that is typically shared by the mated pair. STP mated pairs are geographically separated , This helps ensure protection for message routing they perform if a natural disaster occurs, etc.

9.4 STP TWO-LEVEL ARCHITECTURE IN CCS NETWORK

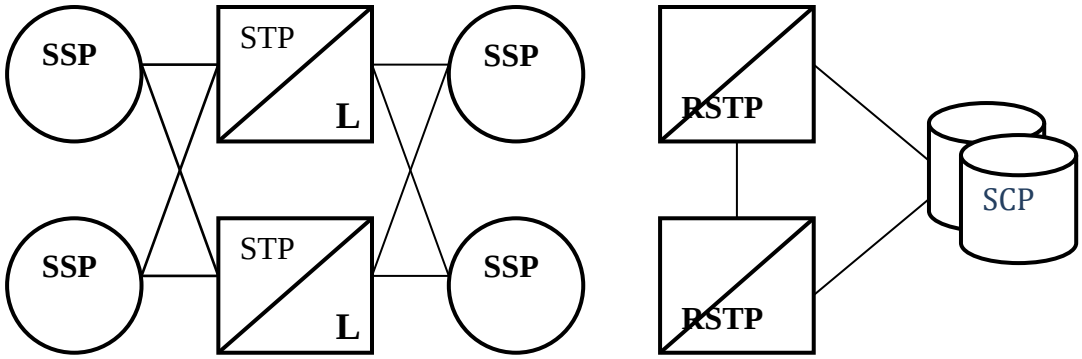


Figure 56: **STP two level architecture**

In large CCS networks, STPs are deployed in a hierarchical arrangement, and typically identified as Regional STPs, and Local STPs.

- There are no functional differences in the two STPs.
- The LSTP handles call set-up and network management traffic within the network.
- The RSTP only handles query traffic within the network requiring access to SCP databases.

STPs are mainly of two types:

- **Integrated STP**

  When STP functionality is incorporated along with 'Service Switching Point' in the 'Service Switching Node', it is known as Integrated Signalling Transfer

Point. It performs call switching functions as well as Signalling transfer functions

- **Standalone STP**
  Standalone STP performs only the core function of SS7 signalling transfer, It enables the operator to manage the network resources in a more effective way and to host more applications.

9.5 SSTP FUNCTIONS

- SS7 Message routing
- Global Title Translation
- SS7 Network Management
- Network Interconnection
- Gateway Screening

9.5.1 SSTP Function – Message Routing

Message Routing: By using outgoing DPC contained in MTP's routing label in a datagram environment (where a separate route may be chosen for each message packet) Routing tables which are prepared to allow message transport between any given pair of SSTPs are stored and maintained within SSTPs. The SSTP's SNM (signaling network management) functions control message routing during periods of link congestion or failure.

- Routing is performed using Destination Point Codes (DPCs) similar to street addresses for the Postal Service. STPs have the ability to route messages to all types of signaling points.
- All nodes in the network are identified by a unique point code. This point code is used by CCSS #7 as the Origination Point Code (OPC) and the Destination Point Code (DPC) in the routing label of all Message Signaling Units (MSUs).

9.5.2 SSTP Function – Global Title Translation

Global Title translation : By using SCCP to translate addresses (Global titles) from signaling messages that do not contain explicit information allowing the MTP to route the message. For (e.g. SSTP translates dialed 1+ 800 number into an SCP's DPC for MTP routing and gives sub system number SSN for delivery of the good data base application at the SCP. When more information is needed to process a call, such as an 800 number, queries are processed for SSPs. STPs contain a GTT table with routing information for the type of query and address of SCP.

9.5.3 SSTP Function – Network Management

Acts as traffic cop to route traffic around failures in a network, and to control link congestion.

TFP Transfer prohibited tells the connecting nodes not to send anything that is destined for the affected node.

TFR Transfer restricted tells the connecting nodes – if all possible, not to send anything that is destined for the affected node.

9.5.4 SSTP Function – Gateway Screening

Screening is the capability to examine Incoming and Outgoing packets and allow those which are authorized. This is done by going through a series of Gateway screening tables that must be configured by the service provider. For example, out of the messages which are coming via a link set only ISUP messages can be allowed whereas on another link only SCCP messages can be allowed by utilizing two basic function allow and block..

Software in SSTPs with inter-network connection is used to control who has access into a Telco's network.

9.6 OBJECTIVES OF SSTP'S

Following were the main objectives:-

- Regulate, measure, and account for inter-network traffic including SMS messages from mobile networks including GSM and CDMA
- Achieve flexibility and transparency in management of signalling for BSNL's wired and wireless networks.
- Optimal expansion of GSM & CDMA network of BSNL
- Introduction of new services.
- Offer CCS7 & IP Signaling Services to other Wireline & Wireless Network Operators.

9.7 STAND-ALONE STP NETWORK

9.7.1 Advantages:

- Dedicated signaling processors, resources
- Upgrade path divorced from MSC / SSP functions, growth
- Most effective method to manage network level resources, features
- Frees up processing capacity from the switches
- Can host most of the applications, centrally
- Full mated pair redundancy

9.7.2 Disadvantages:

- Requires additional investment (However compensated by freeing up extra resources of the switches)
- Requires traffic study, SS7 management

The PO no. P.O.No. SE/PO/005/2016-17/SSTP/New/UTStarcom dtd.01.03.2017 was issued by BSNLCO, for Supply, Installation, Commissioning and Migration to replace the existing SSTP network of M/s.Tekelec (now M/s. Oracle), with a new SSTP network to M/s.UTStarcom India Telecom Private Ltd., Gurgaon. As per the tender and PO, there are total 18 SSTP nodes (with EMS NOC at Bangalore & DR EMS NOC at Mumbai. M/s UTStarcom has supplied all equipment, installed and ATed at all nodes.

9.8 ISG6400

The new UTSTARCOM SSTP iSG6400 primarily implements translation, adaptation and distribution functionality for SIGTRAN and SS7 signaling messages on the bottom layer, and the translation, adaptation and distribution functionality for M3UA-based SIGTRAN signaling、M2UA-based SIGTRAN signaling , SIP and Diameter signaling. The iSG6400 has the following features:

- Flexible Hardware and Software Platforms
- Carrier-Class High Availability
- Powerful System Functions
- MTP Message Screening
- Number Portability
- Diameter Signaling Controller
- Graphical and Convenient Network Management.

BSNL existing SSTP network comprising of 16 SSTP nodes installed in mated pair configuration. The SSTPs at Delhi, Chennai, Pune, & Ernakulum shall be with International Signaling Gateway functionality

Each of the TAXs/IP TAXs & MSCs in BSNL Network shall be connected to at least two SSTPs through IP and/or E1 link per SSTP on load balancing and failover manner

The MSCs in the Indian Telecom Network connected to TAXs/IP TAXs of BSNL Network shall be routed through one of the sixteen SSTPs installed as part of this tender .

SSTPs shall be connected with the BSNL's IP MPLS network through two L3 LAN switches with minimum two GE interfaces The Layer-3 switches shall be deployed in high availability mode (Active-Active) across different arms of each site.

SSTPs shall be interconnected with mated SSTP nodes with FE links /HSL links through the SDH network of BSNL for redundancy purposes in addition to interconnecting the SSTPs amongst themselves and to the EMS locations on the IP MPLS networks. Some network elements are also connected with HSL/FE links. NOC/ DR NOC at Bangalore and Mumbai.

9.8.1 Unique Features Of Utstarcom SSTP :

1. MNP capacity is 250M NP entries and can be further expanded
2. UT SSTP use Oracle DB for eMS and NP DB. Oracle database is a truly carrier-class DB, with high reliability, centralized data management
3. UT SSTP network is composed of distributed SSTP nodes and Centralized eMS/NP SRV /DB SRV, it is more flexible and has a better cost structure. All SSTP node share the centralized DB/eMS/NP SRV
4. Centralized DB means low CAPEX and OPEX
5. Veritas used to synchronize the Oracle DB between different NOC/DR-NOC to implement DB Geographic Redundancy. Veritas is most reliable tools to do this
6. Centralized eMS manages all the SSTP nodes which are deployed around PAN India.
7. eMS is GUI based, easy to operate and use, and more friendly
8. Support SS7 and SIGTRAN
9. Support the emerging DIAMETER AND SIP protocol.

9.9 CONCLUSION

The efficiency of SS7 had made a number of applications possible with e.g. fast connection setup in PSTN, “short message service” and “location update” messages in GSM world. The introduction of Standalone Signal Transfer Point (SSTP) was a historic step from that perspective. It immediately solved issues related to the complexity by converting the mesh networks into the star networks. It is now able to handle the signaling very efficiently. SSTP also handle the non call related messages efficiently. The new SSTPs will be capable of supporting new signaling technologies like SIP and diameter, in addition to existing SS7/SIGTRAN and planned to cater to the signaling needs of BSNL network for future.

10 FTTH TECHNOLOGY & BHARAT AIRFIBER

10.1 LEARNING OBJECTIVES

- Concept of FTTH.
- Network Architecture of FTTH
- GPON and GEPON technology.

10.2 INTRODUCTION

Growing demand for high speed internet is the primary driver for the new access technologies which enable experiencing true broadband. Today's, there is an increasing demand for high bandwidth services in markets around the world. However, traditional technologies, like Digital Subscriber Line (DSL) and cable modem technologies, commonly used for "broadband access," which have access speeds to the order of a megabit per second, with actual rates strongly dependent on distance from the exchange (central office) and quality of the copper infrastructure, can not fulfill today's customer demand for bandwidth hungry applications such as high-definition TV, high-speed Internet access, video on demand, IPTV, online gaming, distance learning etc. Amongst various technologies, the access methods based on the optical fiber has been given extra emphasis keeping into long term perspective of the country. It has many advantages over other competing access technologies of which 'Being Future Proof' and providing 'True Converged Network' for high quality multi-play are the salient ones. The stable and long term growth of Broadband is, therefore, going to be dependent on robust growth of fiber in the last mile.

However, for providing multi-play services (voice, video, data etc.) and other futuristic services fiber in the local loop is a must. The subscriber market for multi-play is large and growing and includes both residences and businesses. Businesses need more bandwidth and many of the advanced services that only fiber can deliver. All view Multi-Play as a strong competitive service offering now and into the future and are looking at fiber as the way to deliver. Optical fiber cables have conventionally been used for long-distance communications. However, with the growing use of the Internet by businesses and general households in recent years, coupled with demands for increased capacity, the need for optical fiber cable for the last mile has increased. A primary consideration for providers is to decide whether to deploy an active (point-to-point) or passive (point-to-multipoint) fiber network.

10.3 FIBER TO THE X (FTTX)

Today, fiber networks come in many varieties, depending on the termination point: building (FTTB), home (FTTH), curb (FTTC) etc. For simplicity, most people have begun to refer to the fiber network as **FTTx,** in which x stands for the termination point. As telecommunications providers consider the best method for delivering fiber to their

subscribers, they have a variety of FTTx architectures to consider. FTTH, FTTB, and FTTC each have different configurations and characteristics.

10.3.1 FTTH (Fiber To The Home):

FTTH is now a cost-effective alternative to the traditional copper loop. “Fiber to the Home” is defined as a telecommunications architecture in which a communications path is provided over optical fiber cables extending from an Optical Line Terminal (OLT) unit located in central office (CO) connected to an Optical Network Terminal (ONT) at each premise. Both OLTs and ONTs are active devices. This communications path is provided for the purpose of carrying telecommunications traffic to one or more subscribers and for one or more services (for example Internet Access, Telephony and/or Video-Television). FTTH consists of a single optical fiber cable from the base station to the home. The optical/electrical signals are converted and connection to the user’s PC via an Ethernet card. FTTH is the final configuration of access networks using optical fiber cable.

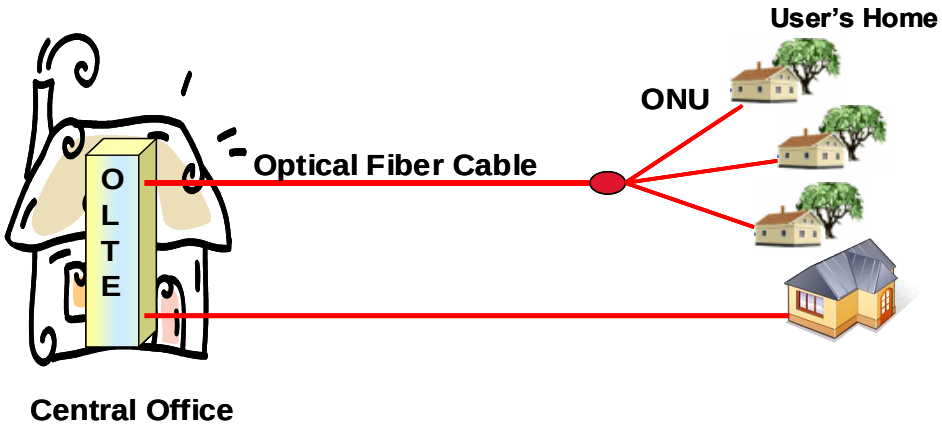


Figure 57: **FTTH Configuration**

10.3.2 FTTB (Fiber To The Building):

“Fiber to the Building” is defined as a telecommunications architecture in which a communications path is provided over optical fiber cables extending from an Optical Line Terminal (OLT) unit located in central office (CO) connects to an Optical Network Unit (ONU at the boundary of the apartment or office or building enclosing the home or business of the subscriber or set of subscribers, but where the optical fiber terminates before reaching the home living space or business office space and where the access path continues to the subscriber over a physical medium other than optical fiber (for example copper loops).

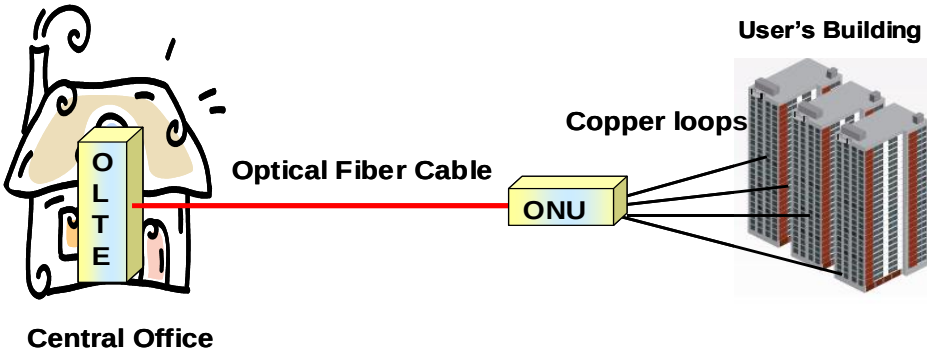


Figure 58: **FTTB Configuration**

FTTB is regarded as a transitional stage to FTTH. By introducing fiber cables from the fiber termination point to the home living space or business office space FTTB can be converted to full FTTH. Such a conversion is desirable as FTTH provides better capacity and longevity than FTTB. Optical fiber cable is installed up to the metallic cable installed within the building. A LAN or existing telephone metallic cable is then used to connect to the user.

10.3.3 FTTC (Fiber To The Curb):

A method of installing optical fiber cable by the curb near the user's home. An optical communications system is then used between the ONU installed outside (such as near the curb or on Street Cabinet) from the installation center. Finally, copper cable is used between the ONU and user.

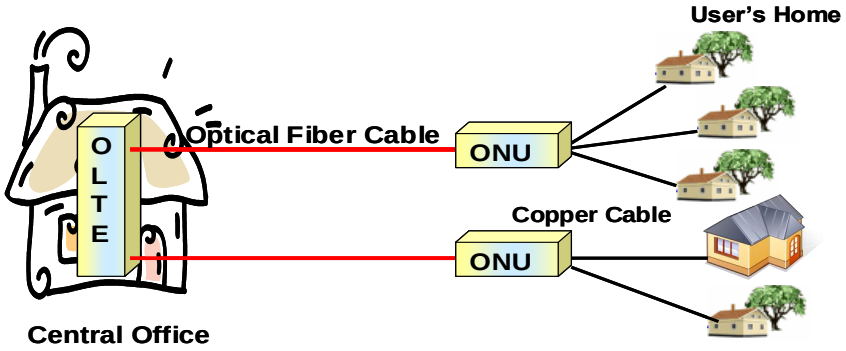


Figure 59: **FTTC Configuration**

10.4 WHY FTTH?

FTTH is a true multi-service communications access which simultaneously handles several phone calls, TV/video streams, and Internet users in the home/office. There are several advantages of deploying FTTH over other traditional access technologies as given below:

- FTTH provides end-users with a broad range of communications and entertainment services, and faster activation of new services.

- Competition is beginning to offer a "multi-play" (i.e., voice, video, data etc) bundle.
- FTTH provides Service Provider's with the ability to provide "cutting edge" technology and "best-in-class" services.
- Deploying a fiber optic cable to each premise will provide an extraordinary amount of bandwidth for future services.
- FTTH provides carriers with an opportunity to increase the average revenues per user (ARPU), to reduce the capital investment required to deliver multiple services, and to lower the costs of operating networks (fewer outdoor electronics, remote management, ..) will result in less operational expense.
- FTTH provides the community in which it's located with superior communications which enhance the efficiency of local business and thus deliver economic advantage for the community.
- Around the world FTTH is viewed as strategic national infrastructure similar to roads, railways, and telephone networks.

10.5 TECHNOLOGY OPTIONS FOR FTTH ARCHITECTURE:

When deciding which architecture to select a provider has many things to consider including the existing outside plant, network location, the cost of deploying the network, subscriber density and the return on investment (ROI). At present different technology options are available for FTTH architecture .The network can be installed as an **active optical network**, or **a passive optical network (PON)**.

10.5.1 Active Optical Network

The active optical network implementation is known as the "Active Node" and is simply described as a "point-to-point" solution. Subscribers are provided a dedicated optical cable and the distribution points are handled by active optical equipment. These active architectures have been setup as either "**Home Run Fiber**" or "**Active Star Ethernet**".

10.5.2 Home Run Fiber (Point-To-Point) Architecture

A Home Run Fiber architecture is one in which a dedicated fiber line is connected at the central office (CO) to a piece of equipment called an Optical Line Terminator (OLT). At the end user location, the other side of the dedicated fiber connects to an Optical Network Terminal (ONT). Both OLTs and ONTs are active, or powered, devices, and each is equipped with an optical laser The Home Run fiber solution offers the most bandwidth for an end user and, therefore, also offers the greatest potential for growth.

Over the long term Home Run Fiber is the most flexible architecture; however, it may be less attractive when the physical layer costs are considered. Because a dedicated fiber is deployed to each premise, Home Run Fiber requires the installation of much more fiber than other options, with each fiber running the entire distance between the subscriber and the CO.

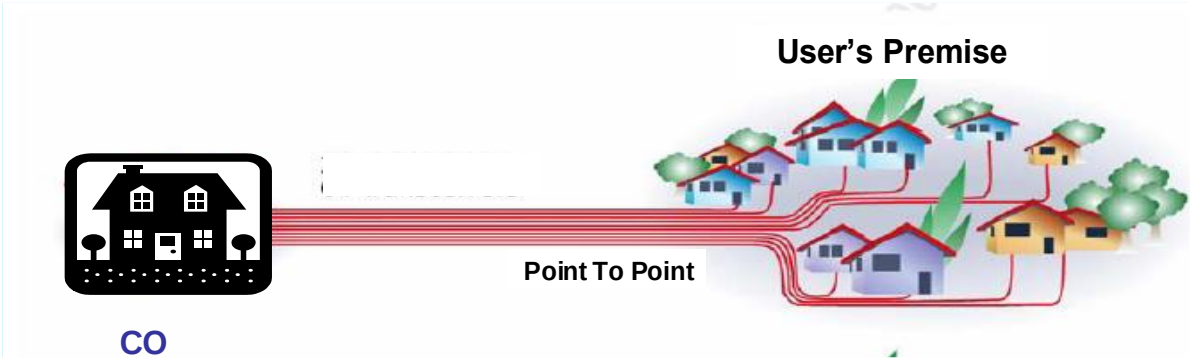


Figure 60: **Home Run Fiber (Point-to-Point) architecture**

10.5.3 Active Star Ethernet (Point-To-Multi Point) Architecture

Active Star Ethernet (ASE) architecture is a point-to-Multipoint architecture in which multiple premises share one feeder fiber through a Ethernet switch located between the CO and the served premises.

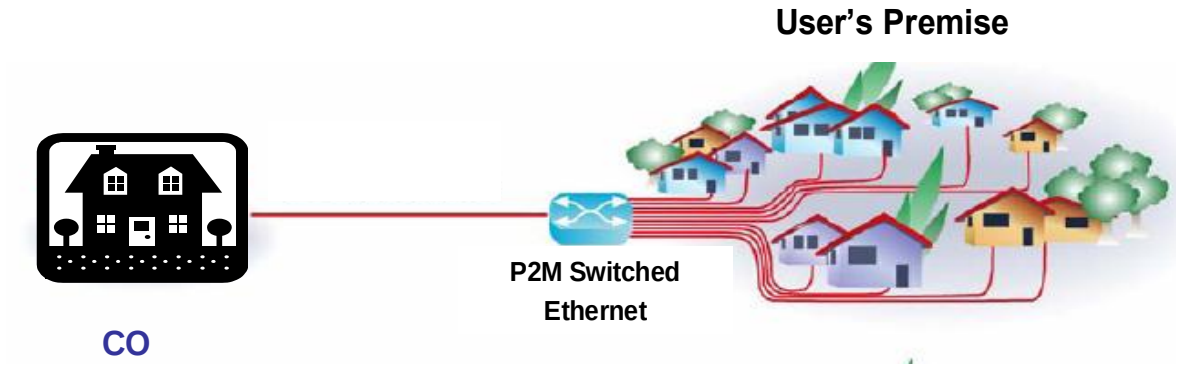


Figure 61: **Active Star Ethernet (ASE) architecture**

With Active Star Ethernet (ASE) architecture, end users still get a dedicated fiber to their location; however, the fiber runs between their location and Ethernet switch. Like Home Run Fiber, subscribers can be located as far away from the Ethernet switch and each subscriber is provided a dedicated "pipe" that provides full bidirectional bandwidth. Active Star Ethernet reduces the amount of fiber deployed; lowering costs through the sharing of fiber.

10.5.4 Passive Optical Network (Point-To-Multipoint) Architecture

The key interface points of PON are in the central office equipment, called the OLT for optical line terminal, and the CPE, called ONU for optical network unit (for EPON) and ONT for optical network terminal (for GPON). Regardless of nomenclature,

the important difference between OLT and ONT devices is their purpose. OLT devices support management functions and manage maximum up to 128 downstream links. In practice, it is common for only 8 to 32 ports to be linked to a single OLT in the central office. On the other hand the ONT (or ONU) devices in the CPE support only their own link to the central office. Consequently, the ONT/ONU devices are much less expensive while the OLTs tend to be more capable and therefore more expensive.

10.6 COMPONENTS OF PON

10.6.1 OLT

The OLT resides in the Central Office (CO). The OLT system provides aggregation and switching functionality between the core network (various network interfaces) and PON interfaces. The network interface of the OLT is typically connected to the IP network and backbone of the network operator. Multiple services are provided to the access network through this interface,.

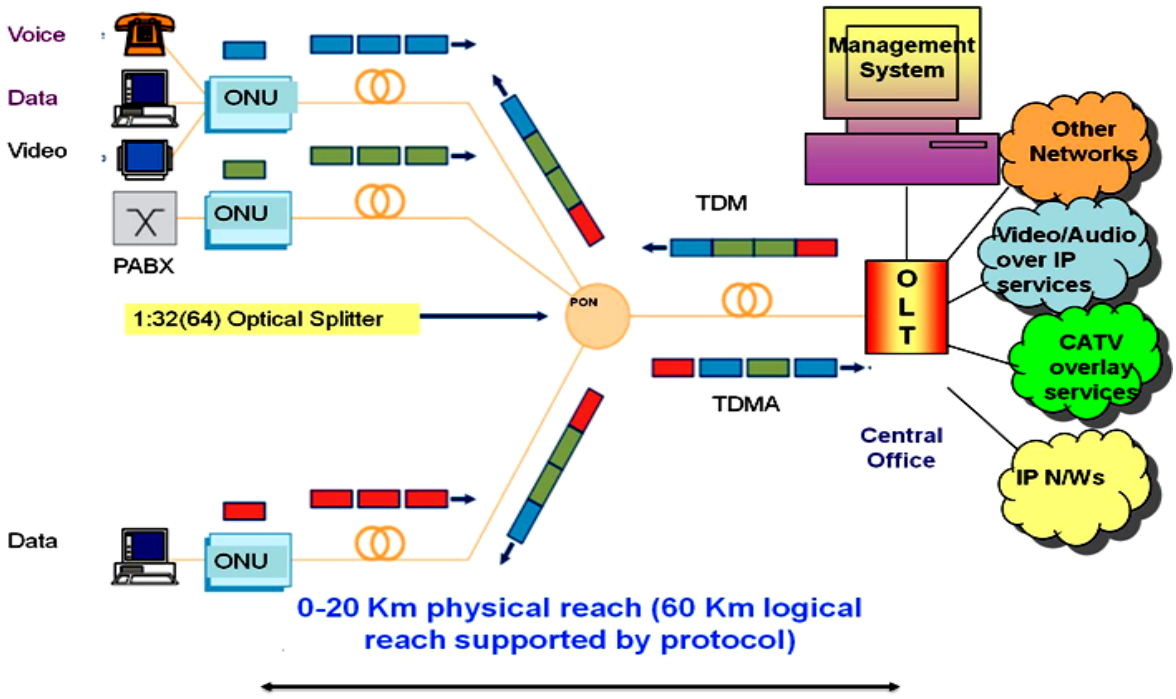


Figure 62: **PON Architecture**

10.6.2 ONU/ONT:

This provides access to the users i.e. an External Plant / Customer Premises equipment providing user interface for many/single customers. The access node installed within user premises for network termination is termed as ONT. Whereas access nodes installed at other locations i.e. curb/cabinet/building, are known as ONU. The ONU/ONT provide, user interfaces (UNI) towards the customers and uplink interfaces to uplink local traffic towards OLT.

10.6.3 Optical Splitters

Distributed or single staged passive optical splitters/combiners provides connectivity between OLT & multiple ONU/ONTs through one or two optical fibers. Optical splitters are capable of providing up to 1:64 optical split, on an end to end basis. These are available in various options like 1:4, 1:8, 1:16, 1:32 and 1:64.

10.6.4 NMS

Management of the complete PON system from OLT.

- One OLT serves multiple ONU/ONTs through PON
- TDM/TDMA protocol between OLT & ONT
- Single Fiber/ Dual Fiber to be used for upstream & downstream
- Provision to support protection for taking care of fiber cuts, card failure etc.
- Maximum Split Ratio of 1:64
- Typical distance between OLT & ONT can be greater than 15Km (with unequal splitting - up-to 35Km)
- Downstream transmission I.e. from OLT to ONU/ONT is usually TDM over 1490 nm wavelength.
- Upstream traffic I.e. from ONU/ONT to OLT is usually TDMA over 1310 nm wavelength.
- PON system may be symmetrical or asymmetrical
- PON and fiber infrastructure can also be used for supporting any one way distributive services e.g. video at a different wavelength

PON is configured in full duplex mode in a single fiber point to multipoint (P2MP) topology. Subscribers see traffic only from the head end, and not from each other. The OLT (head end) allows only one subscriber at a time to transmit using the Time Division Multiplex Access (TDMA) protocol. PON systems use optical splitter architecture, multiplexing signals with different wavelengths for downstream and upstream.

10.7 SPLITTER CONFIGURATIONS

There are two common splitter configurations being used for PON architecture i.e. **centralized and the cascaded** approaches.

10.7.1 Centralized Splitter Approach

The Centralized Splitter Approach typically uses a 1x32 splitter in an outside plant enclosure, such as a fiber distribution terminal. In the case of a 1x32 splitter, each device is connected to an OLT in the central office. In this approach, optical splitters are

concentrated in a single location from which all customer's optical network terminals (ONTs) at 32 homes are connected as shown in fig.63.

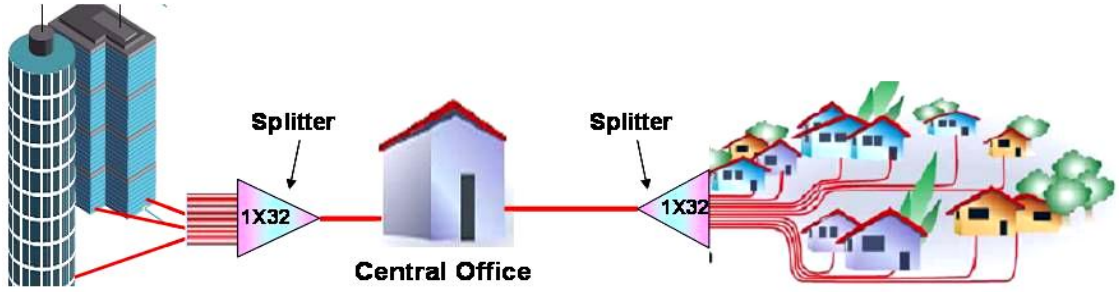


Figure 63: **Centralized Splitter Approach**

10.7.2 Cascaded Splitter Approach

A cascaded split configuration results in pushing splitters deeper into the network as shown in fig.8. Passive Optical Networks (PONs) utilize splitter assemblies to increase the number of homes fed from a single fibre. In a Cascaded PON, there will be more than one splitter location in the pathway from central office to customer. Currently, standard splitter formats range from 1 x 2, 1 x 4, 1 x 8, 1 x 16 and 1 x 32 so a network might use a 1 x 4 splitter leading to a 1 x 8 splitter further downstream in four separate locations. Optimally, there would eventually be 32 fibers reaching the ONTs of 32 homes.

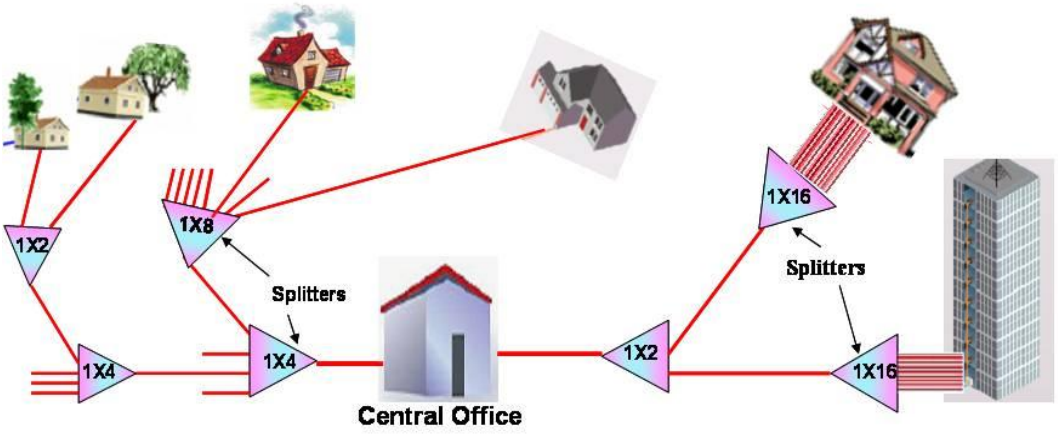


Figure 64: **Cascaded Splitter Approach**

10.8 TYPES OF PON

There are several "flavors" of PON technology, i.e. new access technology named **APON** (ATM Passive Optical Network), **BPON** (Broadband Passive Optical Networking), **EPON** (Ethernet Passive Optical Networking) and **GPON** (Gigabit Passive Optical Networking) which delivers gigabit-per-second bandwidths while offering the low cost and reliability.

10.8.1 APON

ATM PON (APON) was standardized by the ITU in 1998 and was the first PON standard developed. It uses ATM principles as the transport method and supports 622 Mbps downstream services and 155 Mbps upstream service shared between 32-64 splits over a maximum distance of 20 km.

10.8.2 BPON

Shortly after APON, Broadband PON (BPON) followed and is very similar to APON. BPON also uses an ATM, but it also boasts superior features for enhanced broadband services like video. BPON has the higher performance numbers then APON pre-splitting maximum of 1.2 Gbps downstream and 622 Mbps upstream.

10.8.3 EPON

The IEEE standardized Ethernet PON (EPON) in the middle of 2004. It uses Ethernet encapsulation to transport data over the network. EPON operates at rates of 1.25Gbps both downstream and upstream (symmetrical), using 8B/10B encoding over a maximum reach of 20. EPON is also called now as Gigabit Ethernet PON (GE-PON). It is defined as a single fiber network using Wavelength Division Multiplexing (WDM) operating at a wavelength of 1490 nm downstream and 1310 nm upstream. This leaves the 1550 nm window open for other services, such as analog video or private WDM circuits.

10.8.4 GPON

Gigabit PON (GPON) is the next generation of PON's from the line of APON and BPON. The ITU has approved standard G.984x for it. GPON will support both ATM and Ethernet for Layer 2 data encapsulation so is clearly an attractive proposition. GPON supports two methods of encapsulation: the ATM and GPON encapsulation method (GEM). GEM supports a native transport of voice, video, and data without an added ATM or IP encaps ulation layer. GPONs support downstream rates as high as 2.5 Gbits/sec and an upstream rate from 155 Mbits/sec to 2.5 Gbits/sec. BSNL is procuring the GPON that will support downstream rate 2.5Gbps and upstream 1.25 Gbps.

10.9 THE FEATURES OF DIFFERENT PON STANDARD

Features	**BPON**	**GPON**	**EPON**
Responsible Standard body	FSAN & ITU-T SG15 (G-983 Series)	FSAN & ITU-T SG15 (G-984 Series)	IEEE 802.3ah
Bandwidth	Down Stream up to 622 Mbps Up Stream up to 155.52 Mbps	Down Stream up to 2.5 Gbps Up Stream up to 2.5 Gbps	Down Stream up to 1.25 Gbps Up Stream up to 1.25 Gbps
Downstream ג	1490 nm & 1550 nm	1490 nm & 1550 nm	1490 nm
Upstream ג	1310 nm	1310 nm	1310 nm
Layer-2 Protocols	ATM	ATM, Ethernet, TDM over GEM	Ethernet
Frame	ATM	GPON Encapsulation Method	Ethernet Frame
Max. Distance (OLT to ONU)	20 km	20 Km(supports logical reach up to 60 Km)	10 and 20 Km.
Split Ratio	1:16, 1:32 and 1:64	1:16, 1:32 and 1:64	1:16 and 1:32
Line Codes	NRZ (Scrambled)	NRZ (Scrambled)	8B/10B
Downstream Security	**AES:** Advanced Encryption Standard -128 bit key	**AES:** Advanced Encryption Standard (Counter mode)	Not Defined
FEC	None	Yes	Yes
No. of fibers	1 or 2	1 or 2	1
Protection Switching	Support multiple protection configuration	Support multiple protection configuration	None

10.10 PROPOSED SERVICES ON FTTH NETWORK OF BSNL

The first and foremost service proposed in the deployment of these PON technologies is to roll out the **Next Generation Play Network (NGPN).** The following services are proposed on the FTTH network:

- Basic internet Access Service controlled and uncontrolled from 256Kbps to 1000Mbps.
- TV over IP Service (MPEG2).
- Video on Demand (VoD)(MPEG4) plays like VCR.
- Audio on Demand Service
- Bandwidth on Demand (User and or service configurable)
- Remote Education
- Point to Point and Point to Multi Point Video Conferencing, virtual classroom.
- Voice and Video Telephony over IP: Connection under control of centrally located soft switches.
- Interactive Gaming.
- Layer 3 VPN
- VPN on broadband
- Dial up VPN Service
- Virtual Private LAN Service (VPLS)

10.11 BHARAT AIRFIBER

The Bharat Air Fiber services were introduced by Bharat Sanchar Nigam Limited (BSNL) as a part of the Digital India initiative by the Government of India. It is being scaled pan-India. The new service is part of BSNL's plan to provide internet connectivity to rural areas but it differs from its existing BharatFibre service. Bharat Air Fiber Services were inaugurated at Akola in Maharashtra providing the residents wireless internet connections on demand. The aim is to provide BSNL fibre-to-the-home (FTTH) wireless connectivity up to a range of 20 km from the BSNL points of presence.

10.11.1 Features:

- The connectivity speed is 100 Mbps and BSNL is offering various broadband plans in wireline and wireless segments.
- There is a huge demand for high-speed broadband service in the present situation as there is the migration of people from metro cities to rural areas due to the Covid-19 pandemic.
- The service is becoming popular due to Work from Home (WFH), e-learning, online shopping, gaming and entertainment, etc. amidst and after lockdowns.
- BSNL is also providing unlimited free voice calling.

10.11.2 How Bharat Air Fiber Works?

It provides high-speed broadband to subscribers of remote areas by bridging the gap of last-mile connectivity through radio waves.

- A vast network of Optical Fibre has been laid by BSNL up to nearest Telephone Exchange or Mobile Tower and from there the connectivity is provided to subscribers over wireless.
- Bharat Air Fiber service uses the unlicensed spectrum that has not been licensed to any entity as of now. Also, since this unlicensed spectrum has very less interference, the quality of relay is expected to be better for the subscribers in villages where there is very less disturbance for these airwaves.
- It is using line-of-sight radio waves to deploy the Bharat AirFibre and provide call-centre services to the villages. The absence of WiFi routers and appliances like microwave ovens in villages makes them easier for the Bharat AirFibre services to work.

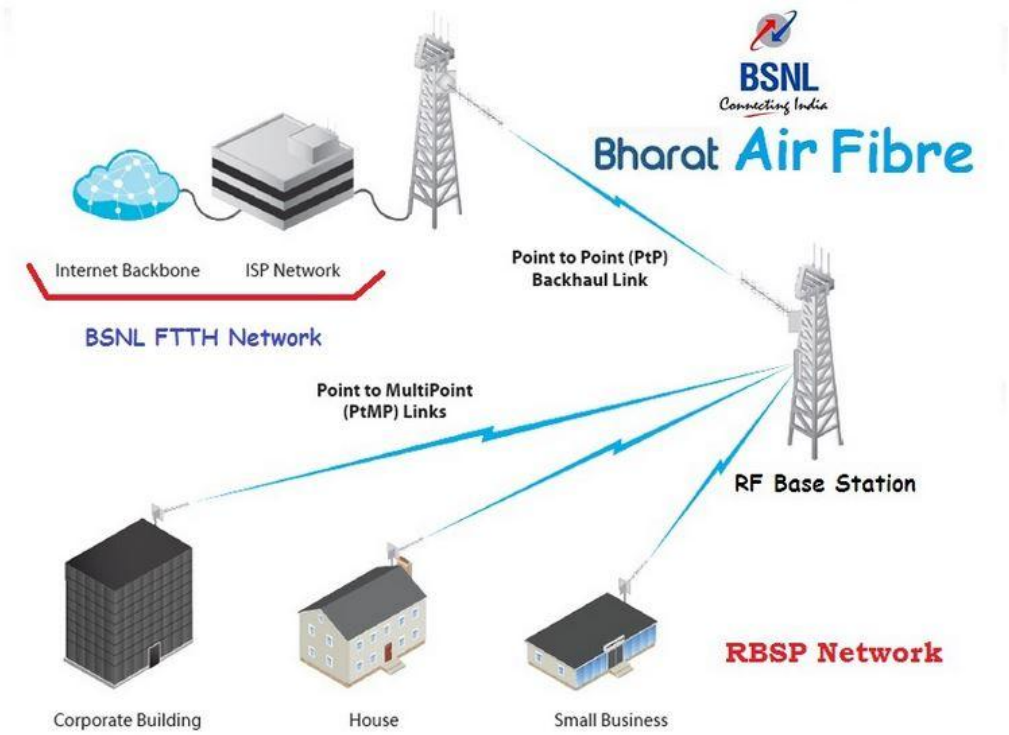


Figure 65: **Bharat Air Fiber Network Architecture**

10.11.3 Benefits

- Customers at remote locations will be benefitted as BSNL comes with the cheapest services with the support of Telecom Infrastructure Partners (TIPs).
- These services are wireless and there are very low chances of interruption in services locally.
- BSNL is tying up with local entrepreneurs/unemployed youth on revenue sharing basis thereby generating employment in rural areas.
- They will earn a regular monthly income of about one lakh per month thereby becoming self-reliant under the Aatmanirbhar Bharat initiative.
- This service could be a game-changer for rural areas as with a little integration of Internet of Things (IoT) and sensors, the moisture content of soil can be known on a real-time basis, so that irrigation can be planned, resulting in saving of water and thereby increasing productivity
- Sensors can be tied to the neck of dairy cattle, enabling continuous recording of body temperature so as to know the exact time when milk output is best.

10.11.4 Bharat Airfibre Is Different From Bharatfibre

The new Bharat AirFibre and BharatFibre sound similar but the latter works is an FTTH service that uses wired technology to provide broadband services while the new AirFibre service is completely wireless. BSNL had started to expand its fibre connectivity in villages with BharatNet and the AirFibre is a continuation of the effort that aims to connect 2.5 lakh Gram Panchayats.

10.12 CONCLUSION

From the BSNL network point of view GPON and GEPON, being the TDM based technology, shall integrate into the existing switching network. BSNL Bharat AirFibre indeed promises to trigger a turnaround in the lifestyle as well as socio-economic quotient of rural India.

11 OPTICAL TRANSPORT NETWORK

11.1 LEARNING OBJECTIVES

- OTN Hierarchy.
- Multiplexing Structure of OTN
- Advantages of OTN
- OTN Interfaces and layer architecture of OTN

11.2 INTRODUCTION

With the growing demand for services and bandwidth, now telecom operators are trying to converge their networks in order to reduce Operational Expenses (OPEX), and also to eliminate additional Capital Expenditures (CAPEX) on multiple parallel networks. The amount of data traffic relative to voice traffic on optical networks and the total traffic volume keeps increasing. These factors are the drivers behind emerging, flexible technologies to supplement the mature, voice optimized, SONET/SDH transport infrastructure and help manage network complexity. The aim of the optical transport network (OTN) is to combine the benefits of SONET/SDH technology with the bandwidth expandability of DWDM. OTN (Optical Transport Network) provides a vehicle to enable convergence, and for providing a common and SONET/SDH-like operational model for network operations, administration, maintenance and provisioning (OAM&P) functionality, without altering the individual services. This newly developed OTN is specified in ITU-T G.709 Network Node Interface for the Optical Transport Network (OTN).

Since the 1980s, SONET/SDH has supported a flexible and transparent mix of traffic protocols including IP, Fiber Channel, Ethernet and GFP by providing protection and performance monitoring. Whilst deployment of dense wavelength division multiplex (DWDM) networks during the following decade served to increase existing fiber bandwidth, it severely lacked the protection and management capabilities inherent in SONET/SDH technology.

The optical transport network (OTN) was created with the intention of combining the benefits of SONET/SDH technology with the bandwidth expansion capabilities offered by dense wavelength-division multiplexing (DWDM) technology.

11.3 WHAT IS OTN?

Networks employing OTN technology are designed and optimized to support current applications employing massive network capacity, and OTN is increasingly recognized as the transport standard of choice to meet the growing demand for network capacity. The ITU Telecommunication Standardization Sector (ITU-T) defines OTN in a set of standards, with the G.709 specification acting as the core technology definition. The ITU-T standards cover the encapsulation format, multiplexing, switching, management, supervision, and survivability of optical channels carrying client payloads. OTN also provides the ability to measure network performance across multiple service providers' domains and to provide seamless, end-to-end monitored services.

An Optical Transport Network (OTN) is composed of a set of Optical Network Elements connected by optical fiber links, able to provide functionality of transport, multiplexing, routing, management, supervision and survivability of optical channels carrying client signals. A distinguishing characteristic of the OTN is its provision of transport for any digital signal independent of client-specific aspects, i.e. client independence.

ITU Standard G.709 is commonly called Optical Transport Network (OTN)– sometimes referred to as **digital wrapper (DW),** allows network operators to converge networks through seamless transport of the various types of legacy protocols while providing the flexibility required to support future client protocols.

OTN provides transport for all digital payloads with superior performance and support for the next generation of dynamic services with operational efficiencies not expected from current optical wavelength division multiplexing (WDM) transport solutions and support for a wide range of narrowband and broadband services like

- · SDH/SONET
- · IP based services
- · Ethernet services
- · ATM services
- · Frame Relay services
- · Audio/Video services etc.

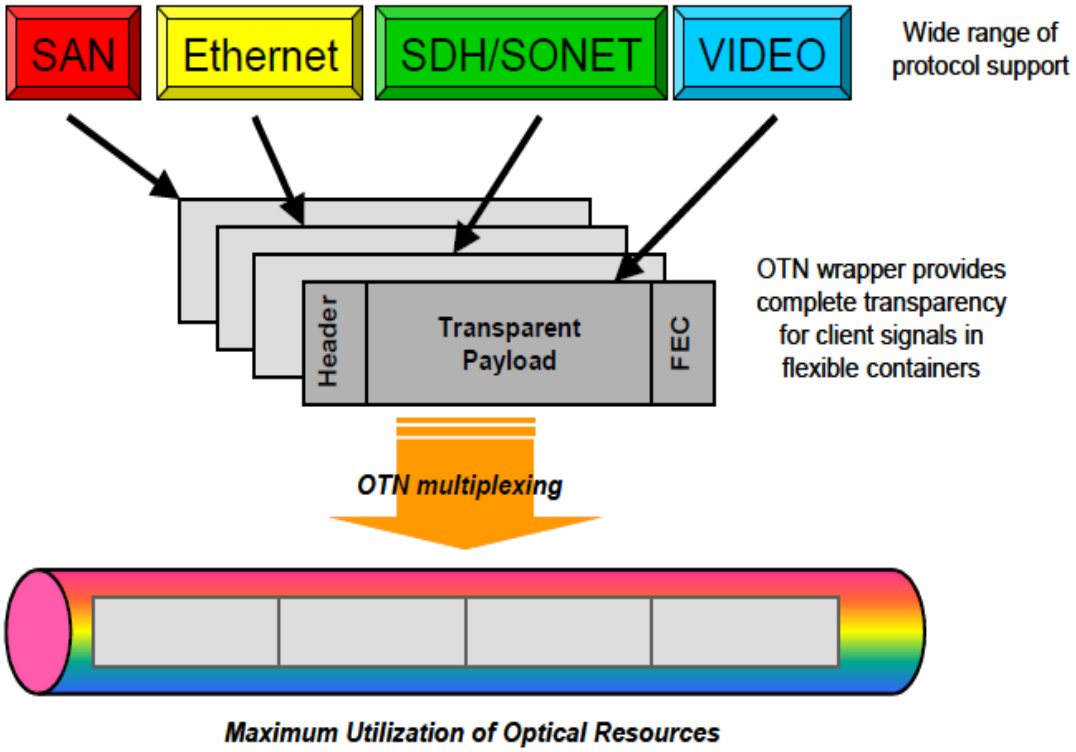


Figure 66: **Converged transport over OTN**

11.4 KEY ADVANTAGES OF OTN

Unlike SONET/SDH, OTN was designed to be an efficient transport layer for packet services such as Ethernet. At the same time, OTN is able to support the multiplexing of many different protocols including SONET/SDH, video, and storage protocols such as Fiber Channel.

OTN offers a number of advantages over legacy transport networks and the primary advantages of OTN include:

- **Reduction in transport costs:** By allowing multiple clients to be transported on a single wavelength, OTN provides an economical mechanism to fill optical network wavelengths.
- **Efficient use of optical spectrum**: otn facilitates efficient use of dwdm capacity by ensuring fill rates are maintained across a network using otn switches at fiber junctions.
- **Determinism:** OTN dedicates specific and configurable bandwidth to each service, group of services, or each network partition. This means that network capacity and managed performance (throughput, latency, jitter, and availability)

are guaranteed for each client, and there is no contention between concurrent services or users.

- **Virtualize network operations:** The ability to partition an OTN-switched network into private network partitions, also referred to as Optical Virtual Private Networks (O-VPNs), provides a dedicated set of network resources to a client, independent of the rest of the network. Each network tenant sees only the resources associated with that tenant's private partition. Other resources associated with other tenants will not be visible. O-VPNs also ease network evolution because network upgrades can be tested or introduced in a protected network partition or 'sandbox,' without the risk of impacting day-to-day network operations in production partitions.
- **Flexibility:** OTN networks give operators the ability to employ the technologies needed now to support transport demands while enabling operators to adopt new technologies as business requirements dictate.
- **Secure by design:** OTN networks ensure a high level of privacy and security through hard partitioning of traffic onto dedicated circuits. This segregation of network traffic makes it difficult to intercept data transferred between nodes over OTN-channelized links. And because OTN-switched networks keep all applications and tenants separate, organizations can effectively stop hackers who access one part of the network from gaining access to other parts of the network.
- **Robust yet simple operations**: OTN network management data is carried on a separate channel completely isolated from user application data. This means OTN network settings are much more difficult to access and modify by gaining admittance through a client interface port.
- **Better Forward Error Correction**: OTN has increased the number of bytes reserved for Forward Error Correction (FEC), allowing a theoretical improvement of the Signal-to-Noise Ratio (SNR) by 6.2 dB. This improvement can be used to enhance the optical systems in the following areas:
- Increase the reach of optical systems by increasing span length or increasing the number of spans.

- Increase the number of channels in the optical systems, as the required power theoretical has been lowered 6.2 dB, thus also reducing the non-linear effects, which are dependent on the total power in the system.
- The increased power budget can ease the introduction of transparent optical network elements, which can't be introduced without a penalty. These elements include Optical Add-Drop Multiplexers (OADMs), Optical Cross Connects (OXCs), splitters, etc., which are fundamental for the evolution from point-to-point optical networks to meshed ones.
- Tandem Connection Monitoring (TCM): TCM enables the user and its signal carriers to monitor the quality of the traffic that is transported between segments or connections in the network.

11.5 OTN VS. SONET/SDH

Although OTN and SONET/SDH have similarities, there are also some significant design differences. Perhaps the biggest difference is that SONET/SDH was defined with fixed frame rates, while OTN was defined with fixed frame sizes.

Table 5. Comparison of SDH/SONET and OTN

OTN	**SONET/SDH**
Asynchronous mapping of payloads	Synchronous mapping of payloads
Timing distribution not required	Requires tight timing distribution across networks
Designed to operate on multiple wavelengths (DWDM)	Designed to operate on multiple wavelengths
Scales to 100 Gb/s (and beyond)	Scales to a maximum of 40 Gb/s
Performs single-stage multiplexing	Performs multi-stage multiplexing
Uses a fixed frame size and increases frame rate to match the client rate.	Uses a fixed frame rate for a given line rate and increases frame size (or uses concatenation of multiple frames) as client size increases
FEC sized for error correction to correct 16 blocks per frame	Not applicable (no standardized FEC)

The G.709 standard defines client payload encapsulation, OAM overhead, FEC, and a multiplexing hierarchy. These functions deliver optical transport capabilities as robust and manageable as SONET/SDH, but with greater suitability for current traffic demands, and data center interconnection circuits in particular.

OTN is asynchronous and thus does not require the complex and costly timing distribution and verification of SONET/SDH. Instead, OTN includes per-service timing adjustments to carry both asynchronous (GbE, ESCON) and synchronous (OC-3/12/48, STM-1/4/16) services. OTN can additionally multiplex these services into a common wavelength.

Like SONET/SDH, OTN also offers comprehensive OAM, but with standardized FEC. OAM is used to efficiently manage network resources and services. FEC enables service providers to extend the distance between optical repeaters, reducing expenses and simplifying network operations.

11.6 OPTICAL TRANSPORT NETWORK (OTN) LAYERS

The optical transport hierarchy (OTH) is a new transport technology for optical transport networks developed by the ITU. It is based on the network architecture defined in various recommendations (e.g., G.872 on architecture; G.709 on frames and formats; and G.798 on functions and processes). OTH combines electrical and optical multiplexing under a common framework. The electrical domain is structured in a hierarchical order just like SONET/SDH, and the optical domain is based on DWDM multiplexing technology but with standardized interfaces and methods to manage the network. ITU-T recommendation G.872, Architecture for the Optical Transport Network (OTN), defines two classes of OTN interfaces:

- ***OTN inter-domain interface (IrDI)***: This interface connects the networks of two operators, or the subnetworks of one or multiple vendors in the same operator domain. The IrDI interface is defined with 3R (reshape, regenerate and retime) processing at each end. Since the IrDI is the interface for interworking, it was the focus of the initial standard development.
- ***OTN intra-domain interface (IaDI)***: This interface connects networks within one operator and vendor domain. Since the IaDI is typically between equipment of the same vendor, it can potentially have proprietary features added such as a more powerful FEC

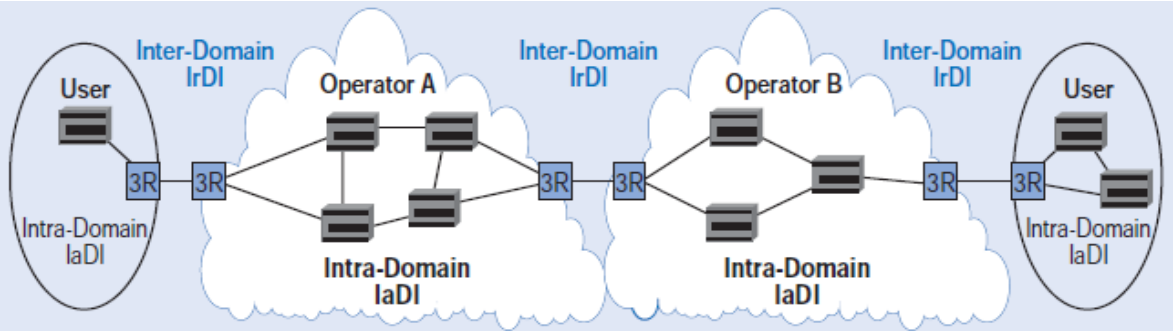


Figure 67: **IrDI Vs IaDI**

The transport of a client signal in the OTN (shown in Figure i.e. Basic OTN Transport Structure) starts with the client signal (SONET/SDH, ATM, GFP, Ethernet etc.) being adapted at the optical channel payload unit (OPU) layer by adjusting the client signal rate to the OPU rate. The OPU overhead itself contains information to support the adaptation process of the client signal. Once adapted, the OPU is mapped into the optical channel data unit (ODU) with the necessary ODU overhead to ensure end-to-end supervision and tandem connection monitoring. Finally, the ODU is mapped into an OTU, which provides framing, as well as section monitoring and FEC.

Additional OH may be added to the OCh to enable the management of multiple colors in the OTN. The OMS and the OTS are then constructed. The result is an OCh comprising an OH section, a client signal, and a FEC segment.

The OCh OH, which offers the OTN management functionality, contains four substructures: the OPU, ODU, OTU, and frame alignment signal (FAS).

Each OPUk (k=0,1,2,2e,3,4,flex) is transported using an optical channel (OCh) assigned to a specific wavelength of the ITU grid. Several channels can be mapped into the OMS layer and then transported via the OTS layer. The OCh, OMS and OTS layers each have their own overhead for management purposes at the optical level. The overhead of these optical layers is transported outside of the ITU grid in an out-of-band common optical supervisory channel (OSC). In addition, the OSC provides maintenance signals and management data at the different OTN layers.

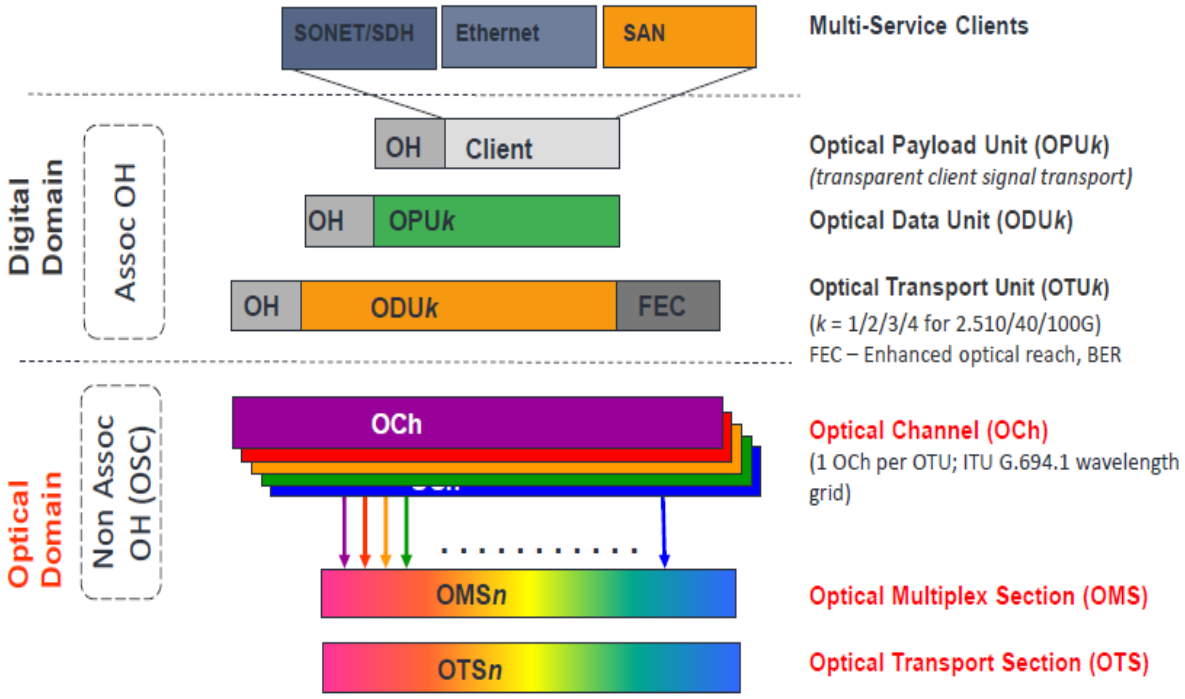


Figure 68: **Basic OTN Transport Structure**

11.7 OTN LAYER TERMINATION POINTS

The ITU G.872 recommendation also defines the optical network architecture based on the optical channel (OCh) carried over a specific wavelength. Different from that of legacy DWDM systems, the structure of this signal is standardized. The OTN architecture is composed of three layers, shown in Figure - OTN Layer Termination Points, and constructed using the OCh with additional overheads.

- **Optical Channel (OCh)** – represents an end-to-end optical network connection with the encapsulated client signal in the G.709 frame structure.
- **Optical Multiplex Section (OMS)** – refers to sections between optical multiplexers and demultiplexers.
- **Optical Transmission Section (OTS)** – refers to sections between any network elements in the OTN, including amplifiers.

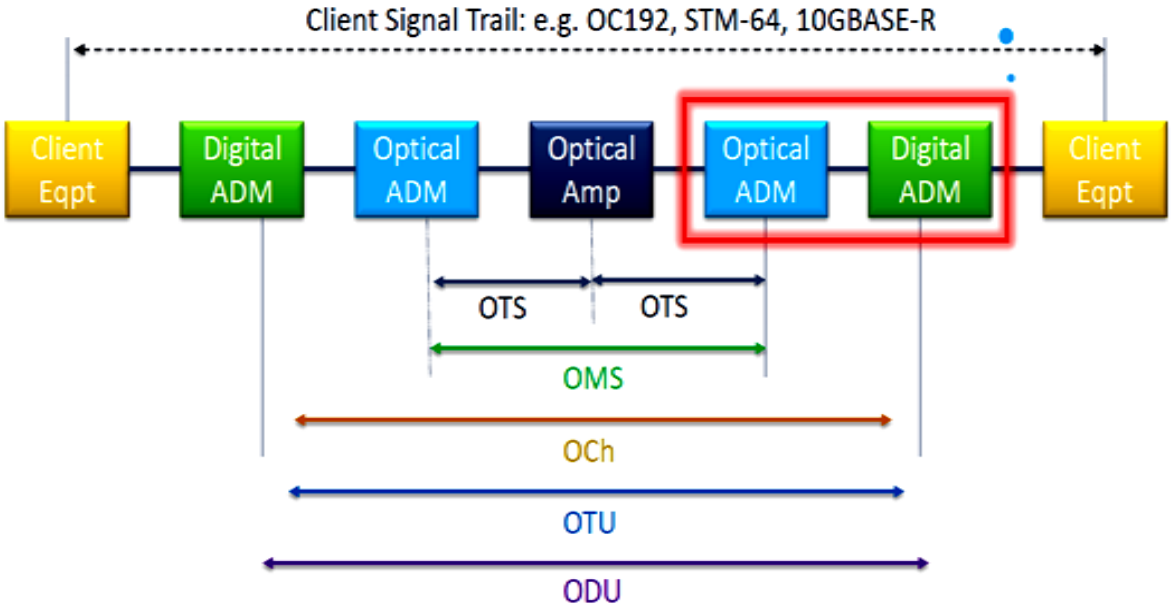


Figure 69: **OTN Layer Termination Points**

The termination of the OTS, OMS and OCh layers is performed at the optical level of the OTN. The OCh payload consists of an electrical substructure, where the optical channel transport unit (OTU) is the highest multiplexing level. This layer is the digital layer — also known as the "digital wrapper" - which offers specific overhead to manage the OTN's digital functions. The OTU also introduces a new dimension to optical networking by adding forward error correction (FEC) to the network elements, allowing operators to limit the number of required regenerators used in the network and in turn reduce cost.

11.8 STANDARD OTN LINE RATES

G.709 defines standard interfaces and rates. OTN rates are equal to or higher than the bit rates of the client traffic. Typical client signals and corresponding to G.709 rates are listed in Table.

Table 6. Standard line rates

Client Signal Type	**Client Signal**	**OTN Line Signal (G.709)**	**OTUk Line Rate (kbit/s)**[	**OPUk Payload Rate (kbit/s)**	**OTUk frame period (µs)**	**OTUk frequency accuracy (ppm)**
SONET/SDH	STS-48/STM-16	OTU1	2,666,057	2,488,320	48.971	± 20
SONET/SDH	STS-192/STM-64	OTU2	10,709,225	10,037,629	12.191	± 20

Ethernet/Fibre Channel	10GBASE-R/10GFC	OTU2e	11,095,727	10,356,012	11.766	±100
SONET/SDH/ Ethernet	STS-768/STM-256/ Transcoded 40GBASE-R	OTU3	43,018,413	40,150,519	3.034	±20
Ethernet	Up to 4 10GBASE-R	OTU3e2	44,583,355	41,611,131	2.928	±20
Ethernet	100GBASE-R	OTU4	111,809,973	100,376,298	1.167	±20
ODUflex signals are transported over ODU2, ODU3, ODU4						±100

Note: ODU0 signals are to be transported over ODU1, ODU2, ODU3, ODU4 or ODUCn signals, ODU2e signals are to be transported over ODU3, ODU4 and ODUCn signals and ODUflex signals are transported over ODU2, ODU3, ODU4 and ODUCn signals

Unlike SDH/SONET, the line rate is increased by maintaining the G.709 frame structure (4 rows x 4080 columns) and decreasing the frame period (in SDH/SONET the frame structure is increased and the frame period of 125 µs is maintained).

11.9 OTN FRAME STRUCTURE

There are three overhead areas in an OTN frame: the Optical Payload Unit (OPU) overhead, the Optical Data Unit (ODU) overhead, and the Optical Transport Unit (OTU) overhead. These overhead bytes provide path and section performance monitoring, alarm indication, communication, and protection switching capabilities. One additional feature is the inclusion of a Forward Error Correction (FEC) function for each frame. The FEC improves the Optical Signal-to-Noise Ratio (OSNR) by 4 to 6 dB, resulting in longer spans and fewer regeneration requirements.

Figure illustrates the three parts that constitute the G.709 OTN frame; **namely the overhead, the payload, and the FEC**.

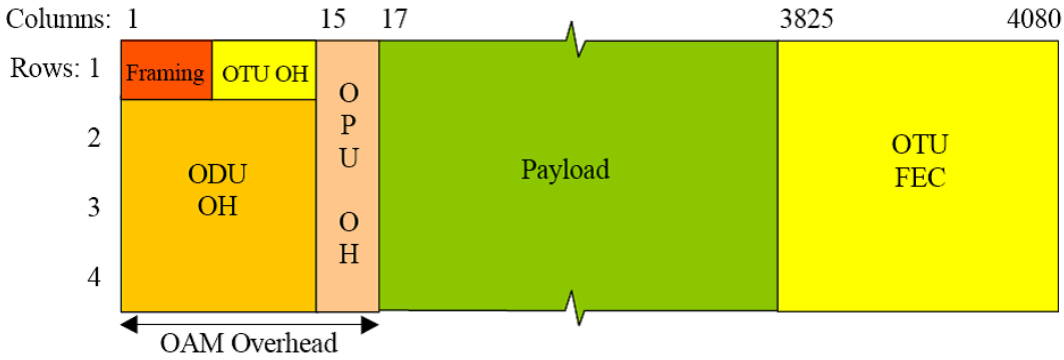


Figure 70: **OTN Frame**

Although OTN and SONET/SDH have similarities but the biggest difference in respect of frame structure is that SONET/SDH was defined with fixed frame rates, while OTN was defined with fixed frame sizes.Perhaps the biggest difference is that SONET/SDH was defined with fixed frame rates, while OTN was defined with fixed frame sizes.

11.10 OPTICAL TRANSPORT NETWORK EQUIPMENT

There are several different types of optical transport network equipment being deployed based on the OTN standards. The most common types include:

- Regenerators,
- OTN terminal equipment
- Optical Add/Drop Multiplexer (OADMs),
- Optical cross connect (OXCs).

OTN terminal equipment is used for point-to-point connections through WDM networks, mapping the client signals into OPUs, sometimes multiplexing multiple signals in the electrical domain, and finally performing mapping/multiplexing in the optical domain. OADMs, OXCs, and some types of regenerators primarily process the OTN signals in the optical domain.

11.11 CONCLUSION

OTN-based backbones and metro cores offer significant advantages over traditional WDM transponder-based networks, including increased efficiency, reliability, and wavelength–based private services. The IP-over-OTN infrastructure also offers better management and monitoring, reduced hops, increased protection of services, and reduced costs for equipment acquisition. In addition to scaling the network to 100G and beyond, OTN plays a key role in making the network an open and programmable platform, enabling transport to become as important as computing and storage in intelligent data center networking.

12 CDR (CRM/ CLARITY)

12.1 LEARNING OBJECTIVES

- Components of a billing system
- CDR based customer care and convergent billing system-project 1 & 2
- Organizational structure of BSNL
- Disaster recovery in CDR project
- Network for CDR project

12.2 INTRODUCTION

The telecommunication environment has become very competitive with multiple operators and multiplicity of services by each operator. In order to be more competitive, companies need to identify customer needs and provide high quality services. The company's ability to provide an accurate and simple bill itself will be an ordeal with the increasing number of services and their complexities. With this demanding requirement and to maintain the competitive edge, BSNL has decided to implement the CDR based billing. This is a big project undertaken by any Telecom service provider in India. It is around 1200 Crore Project.

The implementation of CDR based Billing project will have a number of positive fallouts:

1. **Standardization of systems and processes** - Instead of varieties of systems all over BSNL, a single seamlessly integrated standard operation system will support all the operational activities providing the associated advantages. The overall quality of billing and payment accrual systems should improve.

2. **High quality Customer Care** - The seamless integration will make possible single point high quality customer care.

3. **Paradigm change of CDR based billing -** The shift from call meter base to CDR base will make possible flexible call dependent charging and customer segment based marketing schemes. In addition, this paradigm change in billing will make possible new mandatory TRAI functions such as Carrier selection.

4. **Value added functionalities** - The additional value added functionalities will make possible new powerful functionalities such as formal Revenue Assurance, formal improved CRM, Marketing Campaign Management and so on.

5. **E-Stapling** - Through a special mechanism of E-Stapling, charges of various BSNL services of one customer will be billed together.

6. **Time to Market** – The new convergent billing solution and a services layer built into the integration layer will facilitate the launch of new functionality and

products faster into the market.

7. **Process Efficiency** – New Systems will incorporate Industry best practices that should significantly improve the process efficiency in some of the areas.

The figure shows how a basic billing process works. After a call is made the collector gathers data from the switch and builds a call detail record(Call detail record).The CDR contains the originating number, terminating number, the start time and duration of the call, The CDR is then stored until it can be rated. After rating, the credits and other charges are added. Thereafter the invoices are produced and mailed to the customer in a simple format. Call data is also shared between different service providers which are commonly known as IUC. Issues that must be addressed while managing billing system are reliability, accuracy and readability. Billing different types of services is also a complex issue. To understand the billing process the following figure may be studied.

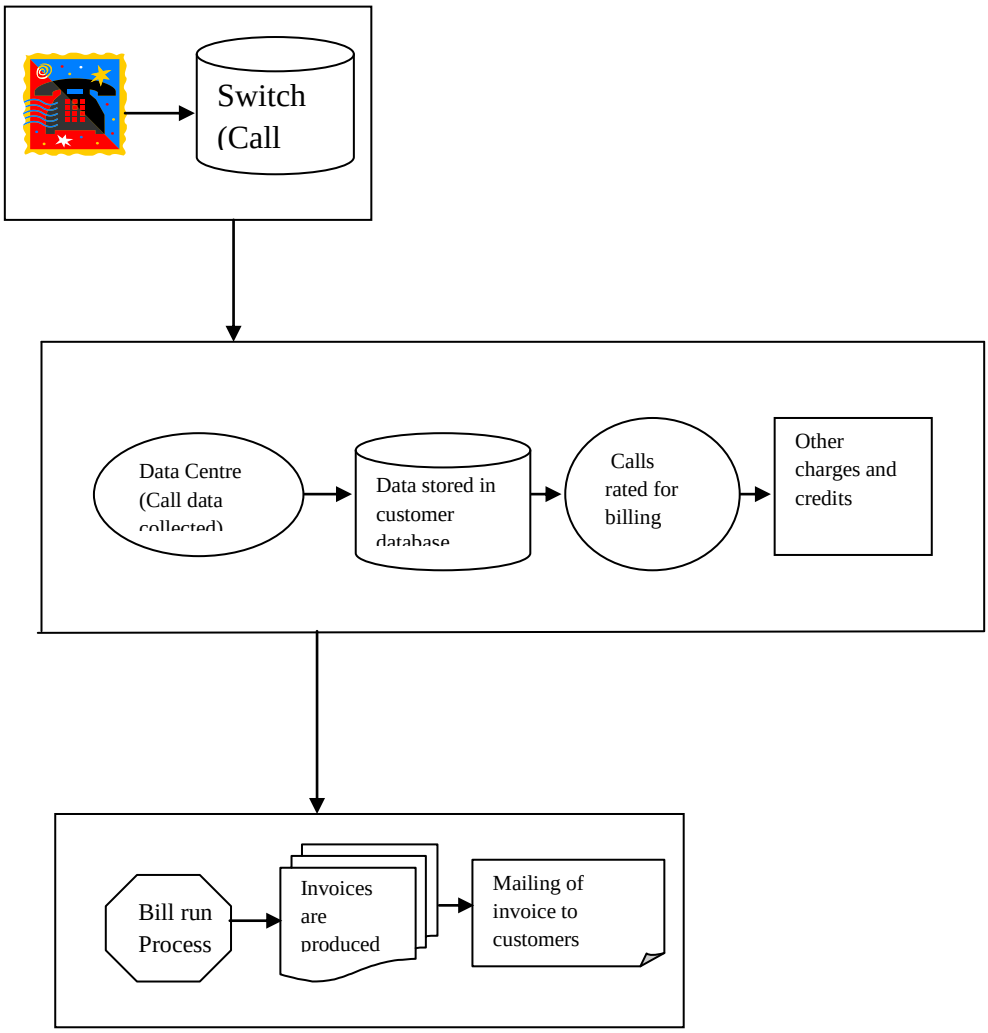


Figure 71: **Billing process**

12.3 COMPONENTS OF A BILLING SYSTEM

A billing system is composed of a series of independent applications that, when run together, are referred to as the billing system. Its major components are as follows:

CDR— This is used to record the details of the call. Usual information on a CDR includes start time of call, type of call, duration of call, originating number, and terminating number. The CDR is stored until time of billing.

Rating application— This matches calls to customer calling plans. The application uses the start, end number, duration, date and time of call to decide what the charge should be, based on the calling plans on the customer's record. This program applies the rate for the individual guided calls. Rating gives the call a value to be charged at the time of billing (not including any promotions, discounts, or taxes).

Billing–This is usually performed once a month. This job collects all of the rated calls that have been stored over the past 30 days. The program adds any promotions and discounts that are associated with the customer account. For example, if customers have called over a certain number of minutes, they might get a volume discount. In addition, taxes and credits are applied.

Formatting -- When the billing job is complete, a file is created that includes all of the customer's information. This file is sent to a print house to be converted to paper invoices. These invoices are then stuffed into envelopes, along with specific inserts targeted to the customer. Many companies will also create electronic statements and send customers their invoices via diskette, tape, or even e-mail; alternative billing practice is especially common for business customers.

12.4 CDR BASED CUSTOMER CARE AND CONVERGENT BILLING SYSTEM-PROJECT 1 & 2

Bharat Sanchar Nigam Limited (BSNL) is having countrywide presence with over 55 million wire line & wireless telephone subscribers and offer hosts of other services like Data communication, National long distance, International Long Distance, Internet, Leased Line, etc. The Company has decided to implement next generation State-of-Art Call Detail Record (CDR) based Customer Care and Convergent Billing System. This assignment involves deployment of Centralized Integrated Billing Systems with supporting technological and communication infrastructure.

Convergent Billing would be based on Call Detail Records (CDRs) obtained from different type of Network elements capable of generating billable information, using centralized Mediation System.

The project enables BSNL to face new challenges due to competition by providing effective and efficient Billing & Customer Care Solutions. It envisages building of country wide intranet, reduce the cost of operation, increase revenue realization, stop

leakage of revenue besides providing round-the-clock best customer care operations.

BSNL implemented the CDR based Billing and customer care solution through out India with four zones and four data centers. This was achieved by carrying out implementation in two zone-pairs each to be referred to as CDR Project 1 and CDR Project 2.

12.4.1 Implementation Plan

The implementation plan is indicated below:

Proof of concept Phase– Setting up of data centers at East-South Zones (CDR Project 1) and North-West zones (CDR Project 2) and implementing all the software solutions along with the networking components meant for the SSAs mentioned below.

Roll out Phase – Implementation of CDR based billing and customer care system in all the remaining SSAs.

The two phases can be summarized as below:

CDR Sub Project	**Data Center**	**CDR Project**	**Proof Of Concept Phase**	**Roll out Phase**
1.1	South	CDR Project 1	4 SSAs (Hyderabad, Bangalore, Thiruananthpuram, Chennai,	66
1.2	East	CDR Project 1	8 SSAs (Kolkata, Patna ,Kamrup, Ranchi, Raipur, Shillong, Puri, Kharagpur)	59
2.1	North	CDR Project 2	7 SSAs (Chandigarh, Ambala, Lucknow , Noida, Dharamshala, Dehradun, Jammu)*	103
2.2	West	CDR Project 2	4 SSAs (Pune, Ahmedabad, Bhopal, Raipur)	83

There would be two different Billing Application Software solutions for the two projects. Scenario is depicted in the table below:

CDR Project 1 (South & East Zones)		**CDR Project 2(North & West Zones)**	
CDR Sub Project 1.1	**CDR Sub Project 1.2**	**CDR Sub Project 2.1**	**CDR Sub Project 2.2**
System Integrator A	System Integrator A	System Integrator B	System Integrator B
HCL	HCL	TCS	TCS

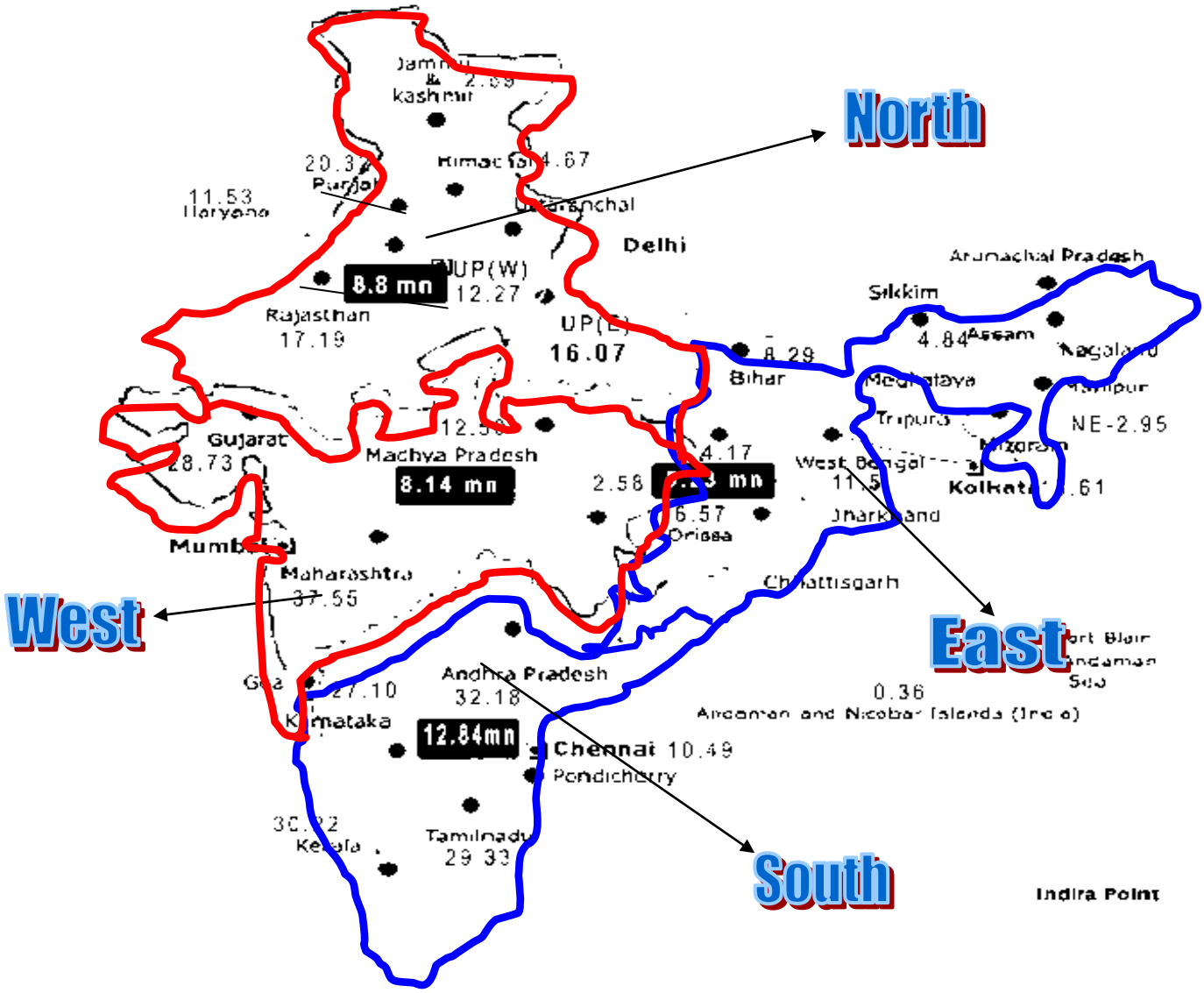


Figure 72: **Approximate DELs**

CDR Project I: Region marked in Blue **(South and East Zones)**	**CDR Project II: Region marked in Red** **(North and West Zones)**

12.5 FUNCTIONALITY

The overall functionality of the system have all the functionalities that were available in the previous packages like DOTSOFT. The commercial, Telecom revenue and accounting and FRS functionalities available in those packages are available in the CDR system also.

This project will replace all the existing systems of Commercial, TRA (Telecom Revenue Accounting), FRS (Fault Repair Service) and DQ (Directory Enquiry).The project will cover the customer care and billing for the following services:

1. Landline
2. Broadband
3. Leased line

The project is not simply a replacement of the existing systems, but it is much more than that. For the first time in the history of BSNL, we are going to have State-of-the-Art Customer Relationship Management (CRM) software. This software will take care of all types of requests from the customers and integrate with other systems such as Order Management and Billing systems.

This software will also provide a Web Self Care (WSC) module, which will enable customers to access the system through the Internet for placing any request, for making payments, or for general enquiry.

12.6 ORGANIZATIONAL STRUCTURE OF BSNL FOR SERVICES

For the purpose of operations and revenue BSNL is divided into circles and each circle is further subdivided into SSAs (Secondary Switching Area).

While circles are typically the same as States, SSAs are same as districts in most of the cases. For the purpose of charging SSA boundary is normally co-terminus with LDCA (Long Distance Charging Area). Each LDCA is further divided into a number of SDCA (Short Distance Charging Area). Headquarter of the SDCA in most cases handles complaints and fault repair service pertaining to the area of SDCA.

Each SSA is like a separate profit centre.

Typically each SSA is responsible for providing service to the customers and subsequent customer support.

Each SSA has both indoor and outdoor staff. Indoor staff is responsible for Network Element maintenance, provisioning, etc while outdoor staff is responsible for building and maintaining the access circuit from NE to the customers premise.

Customer touch points are Customer support centers located in various SDCAs, which are responsible for Service registration and related commercial formalities followed with collection of payments against demand notes and bills.

Back Office operations are offered through commercial offices, accounts offices, operational & maintenance units. Commercial offices are responsible for different kind of service request.

There are well laid out accounting practices which ensures that a proper record is maintained both at the commercial and accounts office for the customer.

Under Zonal Data Centre, BSNL envisages setting up an OSS(Operation Support system) and BSS (Base-station system) infrastructure, which is centralized but has decentralized roles and privileges based access to Customer Service Representatives (CSR) and Account Mangers (all concerned for back office operation) in view of the BSNL's organizational structure described above. Roles and Privileges based access is intended to provide limited access to CSRs/ Account Managers on the system based on different criterion like SSA, Circle and Service center with a permission to carry out one or combination of functions including create, delete, view, print, etc. on different application running at Data Center.

12.7 DATA CENTER

The entire project is going to be implemented with four Data Centre :-

Hyderabad

Kolkata

Pune

Chandigarh

These four Data Centre will take care of all the activities of the Circles in the respective Zones.

Establishment of data centre to host the hardware and software required for all applications. The Network Operation Center (NOC) and Server room shall preferably be located nearby. All Gigabit connectivity between different Data Center equipment shall be on optical / electrical interface. Provision of CCTV based Surveillance System & Access Control System at the Data Center. A separate enclosure shall be provided for monitoring screens

12.8 COMPUTER HARDWARE

Hardware requirement is categorized in two broad levels for all categories of applications.

First category of servers is Connection or Presentation Servers for Applications which are multi instance and scale horizontally. For such a category of applications, Rack mounted Blade Servers/ Rack mounted Stand Alone Servers shall have to used. These type of servers shall be utilized as: EMS Gateways, HTTP servers, SMTP servers, Print Servers, AAA Servers, Logical Security Elements, Network Device Management Servers, DNS Servers, IVRS, Proxies, etc.

Second category is of Datacenter class Servers for the purpose of Database where persistent data is stored and Application Servers where business logic resides within which data is manipulated in response to a client's request. Here database and application

can scale diagonally i.e. scales vertically to an extent and horizontally beyond that. These services can run on multiple mid range servers or on a few high end servers having multiple instances of application running. Following applications shall run on these servers:

Billing and Accounting (Including Rating, OM (if part of Billing) and all other related functionalities), Revenue assurance, Mediation, Provisioning, EAI, CRM (Including CHS, WSC, OM (if part of CRM) and all other related functionalities), Directory Enquiry, EMS, IOBAS,FMS(Fraud Management System), Backup.

Mediation Servers or partitions running Mediation application have X.25 adapters with redundant configuration.. There would be a scenario where X.25 and other types of connectivity are achieved through separate stand alone servers to act as collection server and DC class of Server for further processing. Additional collectors would be configured at each data center for the failover site to take care of 100% collection requirement in DR scenario.

System Architecture would be modular in design allowing future expansions. The Hardware design is done in such a way that there would be no single point of failure. Operational and monitoring tools for each and every hardware system would be provided. Hardware System shall provide status information of the various processes to an industry standard EMS (Third party)

12.9 SOFTWARE

Various software applications with functional modules are Data Mediation System, Billing and accounting, Service Provisioning, CRM & Web Self Care, Directory Enquiry, Revenue Assurance, Enterprise Application Integration, Enterprise Management System, Enterprise Reporting, RDBMS and Security System etc

Customer Relationship Management (CRM) system is the single point customer interface inter-linking Convergent Billing, accounting, commercial, fault control, order and provisioning status, etc. CRM also provides for management of all types of postpaid and prepaid as well as discrete products & services rendered by BSNL. Provision exists for on-line and batch methods of feeding all types of data in each application.

All software modules in OSS are tightly integrated with each other as per BSNL's business requirement. The integration is achieved under EAI (Enterprise Application Interface) framework using industry standard connector/ adapter.

The system is required to be interfaced with existing software application like IVRS, FRS, Billing, Commercial and Directory Inquiry system as per specific need for continuity of the business. Self Care Service through Internet would be provided for identified services by taking due care of system security.

All the software systems would have easy integration capability by supporting industry standard open transport technologies and middleware product. The software systems would offer the capability to import and export information to/from external files or system. The Software System shall support XML and HTML standards for Internet Data Exchange. Software Systems should have capability to apply software or parameter changes without stopping the system.

Software System like Billing, CRM etc would support clear demarcation for the core layer and the customization layer. All business process reengineering would be done through a customization layer. All future versions would have backward compatibility to ensure safe upgrades.

The Software Systems would be able to scale both vertically and horizontally in order to utilize in-box capability of Servers (hardware) and if required by deploying additional Servers.

There would be operational and monitoring tools for each and every software & hardware system.

12.10 DISASTER RECOVERY IN CDR PROJECT

The customer care and billing and other related operations of 334 SSAs are going to be migrated to the four Data Centre. It is very important therefore to have business continuity Plan in case of a disaster.

A disaster is defined as an event that makes continuation of normal functions of a Data Centre impossible. An event could be any one of the incidents like Flood, Fire, prolonged power shut down, strike, earthquake, etc.

In this project, Hyderabad is configured as the DR site for Kolkata and vice versa. Similarly Pune is configured as the DR site for Chandigarh and vice versa. The degradation of performance for the applications failing over to the DR site is permitted up to 50%. This means for example, a billing operation taking 8 hours in the normal course, can take up to 16 hours in case of a disaster.

12.11 NETWORK FOR CDR PROJECT

This project shall implement a countrywide Intranet.This network will connect all SSAs, Circles and the Corporate Office, providing connectivity to all its main exchanges, all officers dealing with customers, such as JTOs, SDEs, AOs, and the entire management.So far, each SSA or Circle has established networks for implementing DOTSOFT and other local systems. This project is going to integrate all the networks and provide a countrywide IP network with MPLS as the backbone. This network will be used not only for implementation of the CDR project, but also for implementing all other IT projects in future, such as ERP.

The following figure shows in general the exchange network and the collection methodology of CDR.

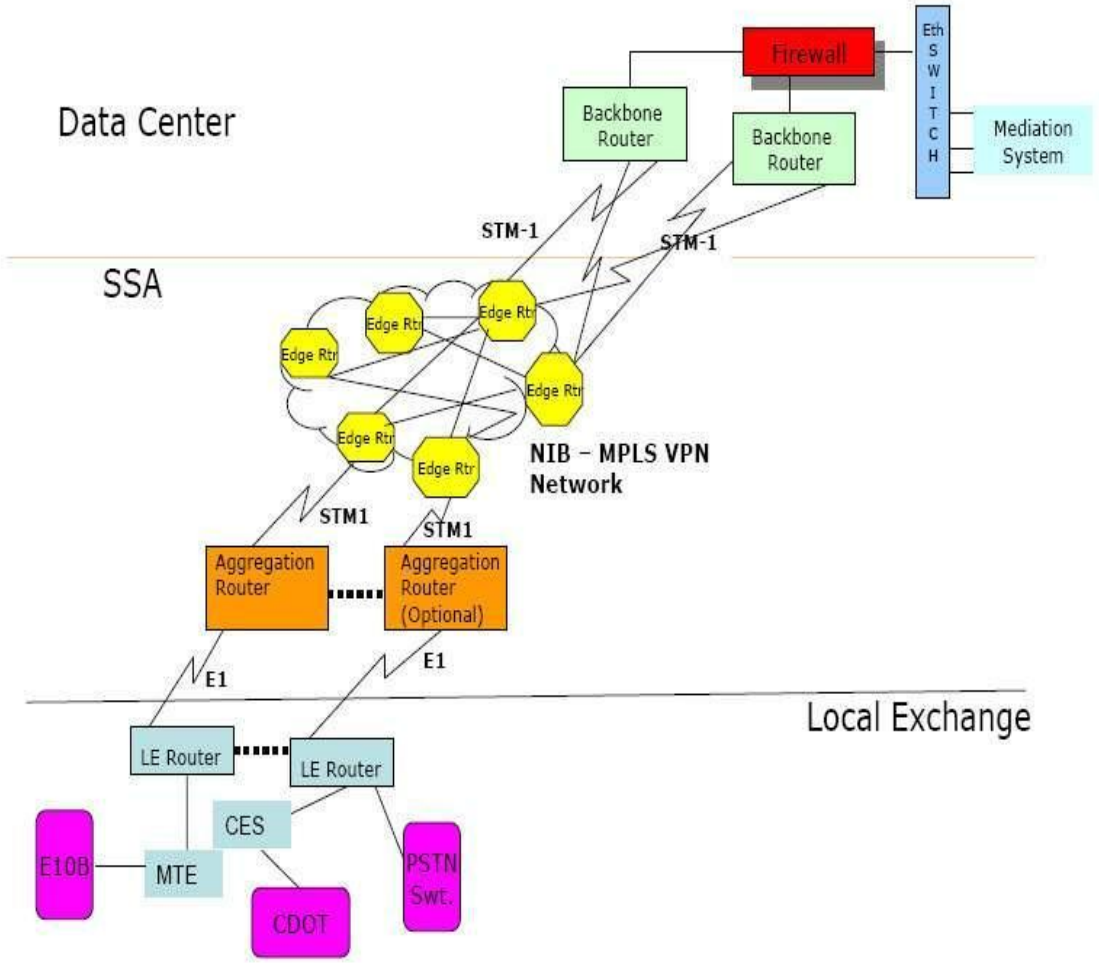


Figure 73: **Network for CDR Project**

12.12 CDR PROJECT CONNECTIVITY TO EXCHANGES

Each exchange is connected to a router, which is called LE router (Local Exchange router). All new technology switches such as OCB, EWSD, 5ESS, AXE, shall be connected using X.25 cards and Ethernet interface (wherever available). All CDOT exchanges will be connected to the LE router using CES equipment supplied by CDOT through HCL. All E10B exchanges will be connected to the LE router through MTE (Magnetic Tape Emulator). Each LE router is connected to the Aggregation Router through E1 links. All the E1s coming from the different exchanges will be aggregated to the Aggregation Router. Each Aggregation Router in each SSA shall be connected over

STM-1 link to the nearest MPLS node. For redundancy purposes, the connectivity shall be established to two MPLS nodes. The Data Centre is also connected to the MPLS network presently through STM-1 links, to start with.This end link will be enhanced to 1 GBPS link or more, later. Thus, each exchange shall be connected to the Data Centre over E1 end links and through the MPLS network.

12.13 CDR PROJECT CONNECTIVITY TO TERMINALS

The existing CSR network will also get connected to the Aggregation Router.Thus, all the terminals of Commercial, TRA, FRS and Directory Enquiry which are now connected to the local systems, will be connected to the Data Centre through the Aggregation Router. The project envisages establishment of new network for collection of CDR from the exchanges, Usage of existing CSR network, with addition of a few CSR, if necessary, And re-utilization of existing PCs in the network.

12.14 CONVERGENT BIILING AND ADVANTAGES

12.14.1 Single Convergent Bill

A customer Account having multiple services with each service having multiple instance shall have option to get single Bill. It shall also be required to give single bill for multiple of such accounts arranged in hierarchy under a Corporate/individual Account

12.14.2 Individual Account

Data consolidation for service and multi instance Customer Account, within a zone, shall be done from existing billing system. Invoice would be generated for each service, the customer has opted for. Individual invoices for a single customer shall be received from different billing system and then a single invoice shall be generated at all four zonal billing centers, after taking in to account bulk discount if any

Extension of Customer care to such customer shall have hierarchical view and the same shall be covered under web self care as well as corporate self care.

12.14.3 Corporate Billing

Three zonal billing centers (South, West and North) and other Billing centers meant for billing other services like GSM based Mobile Telephone, IP Billing, Leased Line Billing, Intelligent Network, etc shall be connected to East Zone to support Corporate Convergent Billing, payment collection etc. In short, BSNL will have multiple Billing System considering multi service environment, which will continue to be in operation even after full commissioning of proposed system. Hence, it is of utmost requirement for the proposed solution to be able to work in conjunction with other Billing system.

The billing system shall be able to collect processed bills from the billing system of following networks existing in BSNL such as MLLN System, CMTS located at 5

different locations, NIB-II, IN System etc

In addition, Billing of Broadband services, CLI based Internet service and other IP services on same landline is also required. In this scenario usage information (rated CDRs) shall be taken from the billing system of NIB-II. CDMA Technology presently deployed in the BSNL network shall be provisioned and billed through the proposed solution.

For Management through Enterprise Management System.

All the APIs for integration with 3rd Party Applications shall be provided.

It would allow the users to use the standby database for read-only access while the synchronization between the primary and standby systems happen simultaneously.

Access to all RDBMS stored procedures shall be available through JDBC, ODBC, C and Active X

Detailed documentation shall be provided for Database Management specific to the project and the applications deployed.

GUI based tool shall be provided to manage, test and tune the database.

All the applications implemented shall have provision for optimizing the number of static connections to the database using connection pooling. All the applications implemented shall also optimize the duration of connection to the database by using techniques like session time out.The database should be able to support partitioning of tables to support linear data scalability and parallel utility processing.

12.15 INTEGRATION WITH IN

BSNL presently offers IN Services like Virtual Calling Card (Brand Name – India Telephone Card), Account Calling Card(ACC), Free Phone, Premium Calling Rate, Universal Access Number, Virtual Private Network, Tele Voting, Universal Personal Number etc. The purpose of integration is to dynamically transfer the Pre-paid amount from the IN Platform to increase in credit limit of a subscriber of a landline to enable bill payment for the post-paid services availed by the subscriber etc. . After integration it would be possible to offer following functionalities:-

The integrated system would have the capability to accommodate for IN and retail customers in a single customer account hierarchy with dynamic transaction guidance from one account to another account in the hierarchy based on service.

The system would have the ability to transfer the balance from IN service like Virtual Credit Card to post-paid service like landline telephone. This will facilitate landline subscriber to pay his retail bills through a Virtual Calling Card which means VCC amounts have to be debited from IN platform and same has to be credited to the Billing System.

The interface between IN Server and Billing Server shall be on secured layer for any transaction. Proven secured protocols shall be used for the purpose.

It shall be possible to redeem loyalty points earned in post-paid service in terms of Virtual Calling Card etc.

All account transaction shall be accompanied with detail log entry in the billing system and the same in readable format may be required to be given to the customers in their normal monthly bills as information.

12.16 CHANGES AFTER CDR PROJECT

- The introduction of this new project will eliminate the need of individual SSAs maintaining and operating TI systems for all the four functionalities, i.e. Commercial, TRA, FRS and DQ.
- The SSAs shall be the end-users of the systems and will have better tools and software at their disposal to provide better customer services.
- The database related jobs would be with the IT team at the Data Centres.
- Change certain business processes within BSNL, a few of them are explained below:

Business processing going to change due to CDR Project

Because of the introduction of new systems and to take advantage of the features of the system, it is proposed to change some Business processes within BSNL that are proposed to change for CDR project

1. Revenue Accounting:
2. Surcharge/Late Fee
3. PCO Billing
4. Deposits
5. Billing Cycles
6. CDR based billing

12.16.1 Revenue Accounting:

In the new system Balance brought forward accounting method shall be used instead of invoice based accounting. For example, a June Bill issued to a customer if not paid, will be added to the July Bill and the July Bill will be issued for an amount, which is equal to both the June and July amounts.

Every customer will be identified by an Account Number, which shall be unique throughout the country. Revenue booking shall be based on the Account even though the services under the account are scattered across the various SSAs. The customers can pay

any amount at any time and it shall be credited to the account and adjusted against the outstanding

12.16.2 Surcharge/Late Fee

Surcharge will be treated as a late fee, which will be a percentage of the outstanding instead of at the slab rate as is being done today. The late fee concept is already introduced in the GSM billing system and the same shall be followed here.

12.16.3 PCO Billing

For PCO billing, the commission payable and the minimum guarantee will be as per the billing cycle instead of on a monthly basis. PCO operators are now eligible for discounts instead of commission. These changes are already done in the existing systems and shall be continued in the new system.

12.16.4 Deposits

Deposits are already made uniform i.e. Rs.500/- for Local, Rs.1000/- for STD and Rs.2000/-for ISD. This shall be common for all the Plans. Therefore, we shall not be offering any OYT or TATKAL deposits/schemes. The existing OYT subscribers shall continue to be billed till the completion of 20 years. However, no new OYT connection shall be provided.

12.16.5 Billing Cycles

The number of billing cycles in an SSA may increase. The new system is going to have a centralized billing process common for all the SSAs in a zone.Therefore, the customers in the entire zone shall be divided into different billing cycles to evenly distribute the process load on the servers.

The number of billing cycles may even go up to 15 once the project is rolled out in all the SSAs.

12.16.6 CDR Based Billing

The existing tariff, which is based on MCUs and number of calls, will get migrated to MOU (Minutes of Usage) based system.

The discounts may be given not in terms of Free Calls, but shall be in terms of Free Talk Time given as Minutes per month or Rupees per month. Though the system offers lot of flexibility in configuring different Plans, BSNL in turn may have to follow certain discipline in offering various Plans to the customers.

It is proposed to authorize the Circle Office team to configure the plans as per business requirements and in future SSAs may not be able to configure new Plans on their own. Each Plan shall be identified by a Plan Code in the system.This discipline will help the organization in monitoring the launch of tariff Plans across the country and it will help BSNL to take correct business decisions.

The products and services that would be supported by the new billing system would be

Wire line Services: Basic Telephony (PSTN), National Long Distance, International Long Distance, ISDN, ATM and IP Services, IN services like Free phone, VCC, ACC, Premium rate services, etc.), Leased lines, E1/ ISDN-PRI (in the context of reverse charging).

Wireless Services: GSM – (Pre-Paid and Post-Paid), GPRSWAP on Mobile including applications like - mobile banking, weather update, news update, Stock update, Travel guide, etc

Data Services: Data calls, IP packets, Content Delivery, Internet services (including VoIP), Fax over IP (FoIP), E-mail services, Video on Demand (VoD), Video & audio conferencing, Internet Roaming

Other Services: Unified Messaging Service, Short Messaging Service, Voice Mail Service, INMARSAT, VSAT, Hotline, IVR based customer service, Virtual Private Network (VPN), xDSL access services, QoS, Frame Relay

Call Management Services: Caller Line Identification Presentation & Restriction, Call Waiting, Call Barring, Call Forward, Call Conferencing, Call Transfer, Malicious Call Tracking,

Miscellaneous requirements Ability to bundle services and the associated default products into one unit so as to make it easy for the CSR to associate it to the Subscription / Customer, Ability to support Number Portability, Grouping of DELs like in ISDN, Level DID, There shall not be any limitation on specifying the number and types of categories for any type of service. For eg. for fixed line services there can be tens of categories such as Residential, Commercial, SME, etc. Similarly there can be sub-categories in each service type eg. In leased line service there may be 64 kbps, nx64 kbps etc.

12.17 CONCLUSION

In the competitive era of telecommunication, telecom companies need to identify customer needs and provide high quality services. The company's ability to provide an accurate and simple bill itself is a challenge along with the increasing number of services and their complexities. With this demanding requirement and to maintain the competitive edge, BSNL has implemented the CDR based billing. Instead of a variety of systems all over BSNL, a single seamlessly integrated standard operation system of CDR will support all the operational activities providing the associated advantages.

13 CSC AND VARIOUS SALES CHANNELS

13.1 LEARNING OBJECTIVES

- Explain the Internal and External Sales Channels of BSNL.
- Explain the Role of Internal sales channels (CSC).
- Explain the Role of External sales channels.

13.2 INTERNAL SALES CHANNELS (CSC)

13.2.1 Service Offered By Bsnl CSC

1. Mobile service- BSNL CSC is providing mobile service in form of New connection, SIM replacement, Re-connection, Customer records updation, C-TOP UP, recharge, mobile number porting & post paid customer's service etc.
2. Landline Service- BSNL CSC is also providing Landline service in form of New connection, shifting, Plan change, Disconnection etc
3. Broadband service
4. FTTH service
5. BSNL Wings service
6. Supporting DSA & Franchisee for expanding business through outdoor sales channels.

13.3 EXTERNAL SALES CHANNELS

1. Franchisee
2. e-Distributor
3. DSA
4. Rural Distributor

13.3.1 Franchisee

Franchisee will be responsible for selling all BSNL to BSNL subscribers. Products, directly or through Rural Distributors (RDs) / retailers within a defined territory. To facilitate retailers, provision of three tier structure has been made by including Rural Distributor between franchisee and retailers only in rural territories to serve the area within the rural BTS.

13.3.1.1 Responsibilities of Franchisee

a) Selling of all BSNL Products purchased by Franchisee directly or through Rural Distributors (RDs) or retailers.

b) Two tier structure for urban and three tier structure for rural areas by incorporating intermediate channel of RDs.

c) Franchisee to make best efforts to actively market and promote the BSNL Products as permitted by BSNL.

d) Franchisee must appoint sufficient numbers of retailers in the territory.

e) Retailers in the rural areas will be appointed and served by RDs.

f) Meeting all sales targets set by SSA/Circle for the franchisee territory.

g) CAF collection, documentation (physical documentation as well as electronic documentation) and timely submission of documents to BSNL as per regulatory guidelines and BSNL instructions.

h) Verification of credentials of customers – Verification of POI/POA (photo, identity and address) of customer at the POS (Point of Sale) has to be done as per the various guidelines issued by DoT and BSNL from time to time.

i) BSNL reserves the right for CAF entry/CAF collection/CAF submission through any third party on outsourced model.

j) Operation of IT tools and systems provided by BSNL as specified from time to time, including hiring data entry operator if required.

k) Appointing required number of FoS (Feet-on-Street) exclusively for BSNL Products to serve retailers as per guidelines in force.

l) Assist and cooperate with the Franchisee Manager or any other BSNL employee appointed by BSNL in respect of sale of BSNL products, and provide him/her with the required details as specified by BSNL.

m) Providing List/Details of FOS and retailers to BSNL.

n) After sales services to end-customers in its own capacity and at its own cost, which shall include receiving, attending & rectifying complaints.

o) All forms of complaint handling on phone and walk-in-complaints (hardware related, billing, service, performance related etc.) will be handled directly by the Franchisee.

p) Serving retailers and Rural Distributors at their doorsteps.

q) The margin/ discount/ incentives / commissions extended by BSNL to franchisee and eligible retailers in their chain/ network

r) Receiving advertisement/ marketing material from BSNL, and displaying it at POS and distribution to Rural Distributors.

s) Promotion of BSNL Products at Franchisee‟s own cost.

t) Arranging special promotional events, as per BSNL requirements, at Franchisee‟s own cost, which shall include events and camps/canopy in unreached and potential areas.

u) Timely submission of bills and claims to the nodal officer .

v) Storage of SIM‟s, data cards and other telecom products purchased by the Franchisee from BSNL in a proper manner.

w) Provide all necessary information to BSNL including but not limited to its books of accounts, or any other information for the purpose of submitting the same in any proceedings before any Government Authority or against any third parties.

x) Issue receipts: At the time of booking of any new connection, franchisee shall issue its formal receipt / invoice to the Rural Distributors (RDs) / retailers.

y) Franchisee will be responsible for all the work done through its distribution network.
aa. The franchisees will be responsible for intimating their GSTN No. to BSNL for billing purpose.

13.3.1.2 Responsibilities of BSNL

a) Appoint sufficient number of Retailer Managers, Retailer Manager Coordinator (RMC), and Franchisee Managers for providing time-to-time guidance, and addressing issues/ concerns raised by franchisees.

b) BSNL shall communicate to the Franchisee the minimum sales required to be made by them on quarterly/ monthly basis, in order to remain eligible for the Franchiseeship Agreement

c) Resolution of issues (including supply of SIMs, payments, servicing of retailers, cross-selling, etc.) raised by franchisees, rural distributors, franchisee managers, RMC, retailer managers, retailers and any other member of the Sales & Marketing team.

D) It will be the responsibility of the Account Officer to remit the collection from the franchisee to credit to Company’s account on as and when purchases of BSNL Products (except post-paid products) are made by the Franchisee and ensure realization of the cheque.

e) The cheque deposited by the Franchisees should be deposited with bank for realization in a manner that it is realized latest by 3rd day (Date of purchase + 2 working days). The Account Officer shall be responsible for ensuring collection, deposit with the bank and realization of the cheque(s).

f) Franchisee manager / SSA Sales Head (Mobility) to ensure that all sales made by BSNL to franchisee and is recorded in BSNL specified IT system.

g) The Sancharsoft & stock register giving details of material sold to the Franchisee should be properly maintained and monitored on regular basis by SSA Sales Head (Mobility).

h) MRP of the products should be displayed. The stocks and distribution of publicity materials like brochures etc., preferably in local languages also should be available in sufficient quantity.

i) In order to promptly receive CAFs, there should be at least one desk counter, totally dedicated to accept CAFs from Franchisees/DSAs at a prominent location in every city and should be manned on all days, including holidays.

j) Ensure timely payments to all channel partners preferably online.

k) It will be mandatory on monthly basis to reconcile the account of prepaid product along with IN report.

l) The following items shall be given free of cost to franchisees for performing their responsibilities, including for demo purpose, and are not linked with the sales targets to be made by the franchisees:

- One rent free landline connections with unlimited on net local calls (LL + Mobile) within circle.
- One rent free landline connection for incoming calls with Broadband plan – BBG Combo ULD 850 (350 monthly free call with unlimited download/Upload).
- One rent free VPN over Broadband (512 kbps VPN BB plan)
- One rent free GSM post-paid Plan – 525, calls beyond freebies shall be payable.
- Ensure alternate/standby media connectivity to Sanchar-Soft terminals working with franchisees.

13.3.2 E-Distributor

BSNL is serving customers through Franchisees/ Rural Distributors/ DSAs/ Retailers in the defined geographical area. To serve the customers through web portal/ Kiosk/ ATMs/POS (Retailers) and other electronic modes. There is a need to appoint Zonal level franchisees and will be known as e-Distributors.

To serve BSNL customers through web portal / Kiosk /ATMs /POS (Retailers) and other electronic mode, there is a need to appoint Zonal Level franchisees to be known as e-Distributors. There will be three types of e-Distributors:

I. Cat -1 : who is applying for single zone

II. Cat -2 : who is applying for two zones.

III. Cat-3 : who is applying for all four zones i.e. on PAN India basis

Following key features are there for e-Distributor Policy

a) e-Distributors have to sell e-recharge/ top-up to prepaid connections and / or postpaid bill payment and / or other BSNL products purchased by them from BSNL, from time to time through web based platform / Kiosk /ATMs/ POS (Retailers) using Internet /API / mobile apps/ data access or other electronic modes.

b)e-Distributor and BSNL shall act on a principal to principal basis and at no time, the distributor shall act in the capacity of an agent of BSNL.

c) The e-Distributor shall be responsible for investment in setting up requisite infrastructure viz. Outlets, portals, servers, leased connectivity etc.

d) e-Distributor shall integrate its system with BSNL‟s zonal C-top up systems and will ensure security of data link by way of Firewall/ IDS etc. C-top up vendor will share APIs for the integration purpose.

e) The reports needed by BSNL for reconciliation and monitoring purpose will have to be developed by both parties and will be validated by BSNL team appointed by the GM (CMTS), Nodal Center before start of actual application.

f) A secured password based account shall be created for BSNL to facilitate remote login to the server by designated BSNL staff. BSNL shall be permitted to view all reports and track sale and distribution to the EFTPOS terminals/NET/SMS.

g) Messaging facility shall be provided between the central server and the EFTPOS terminals wherein BSNL shall be able to pass on marketing related information, special promotional schemes etc to the EFTPOS terminals.

h) The e-Distributor shall store all records of sale at the Central server for a period of at least one year to enable tracking of Sale etc by Law enforcement agencies in India.

i) BSNL may from time to time provide information, training and assistance relating to the services.

j) BSNL may provide the marketing material to the e-Distributor.

k) BSNL shall not be liable for any loss, pilferage or damage to the goods stored and sold at the premises and the merchandise shall be the entire responsibility of the e-Distributor.

13.3.3 DSA

The Direct Selling Agent shall market and sell all BSNL Products to customers at their door steps.

BSNL and DSA shall observe the following procedure in connection with purchase and sale of BSNL Products:

a) The DSA shall place an order for purchase of products from BSNL.

b) Upon dispatch of ordered products, BSNL shall raise an invoice on the DSA, net of applicable discount to be provided to DSA

c) BSNL will charge GST on the price at the transaction value i.e. the price at which BSNL sells its products to DSA. BSNL would raise the sale invoice for sale of BSNL products to DSA.

d) GST paid by DSA to BSNL shall be available to DSA as input tax credit which can be set off against the GST charged by DSA to the retailer

e) v. Secondary / subsequent incentives such as incentive on FRC/RC, any scheme based incentive, FOS incentive etc. to DSA shall be given online in the form of c-top-up value through any platform like Sancharsoft/Pyro/ERP after levy of applicable taxes i.e. TDS /GST etc, wherever applicable.

f) For the subsequent incentives provided by BSNL (refer point 18 above), DSA will raise an invoice (along with applicable GST) on BSNL. Since incentive is paid to DSA in the form of c-topup, BSNL will also raise an invoice (along with applicable GST) on DSA for allocation of such c-topup value .

g) Where DSA is not registered under GST Act, it shall be the responsibility of BSNL to discharge liability under reverse charge mechanism. It is further agreed that DSA shall not charge tax on invoice .

h) BSNL shall, withhold tax at source under Chapter XVIIB of the IT Act, 1961 on the secondary/ subsequent incentive provided by BSNL to the DSA for sale of BSNL Products .

i) GST paid by DSA to BSNL and by BSNL to franchisees (as the case maybe w.r.t. secondary / subsequent incentive provided by BSNL) shall be available to DSA and BSNL, respectively, as input tax credit which can be set off against the GST charged by DSA or BSNL x. Methodology and applicable tax deduction/reconciliation on payment like discount at the time of sale of BSNL Products, discount on FRC/RC, any scheme

based incentive, FOS incentive etc. to DSA may be changed time to time & necessary instructions shall be issued by concerned cell of BSNL CO.

j) The invoices raised by DSA and BSNL should comply with all the conditions as prescribed under the tax invoice rules under Central Goods and Service Tax Rules, 2017.

k) Where DSA is not registered under GST Act, it shall be the responsibility of BSNL to discharge liability under reverse charge mechanism.

l) Applicable Tax deductions/ reconciliation/ accounting related instructions/ guidelines shall be issued by concerned cell of BSNL CO, which shall be applicable to circle/SSA.

m) Rate of discount/ margin/ incentive needs to be reviewed with every change in the rate of GST in order to keep it at par with or lower than the current rate applicable on face value.

n) Methodology of calculation of discount/ margin, Applicable Tax deductions/ reconciliation/ accounting related instructions/ guidelines shall be issued by concerned cell of BSNL CO will be issued from time to time, which shall be applicable to circle/SSA.

o) In case of any deviation, default or negligence on the part of DSA due to which it is liable to pay penalty to BSNL, the same shall be recovered by BSNL from DSA along with applicable GST tax (as may be applicable)

p) BSNL shall deduct tax at source if required under GST Act and GST regulations, any law or any regulation.

q) In case of any deficient supply or incomplete supply, it shall be the responsibility of DSA to issue GST compliance credit note (both at the time of sale of BSNL products or at the time of subsequent incentives provided to the DSA)) within the reasonable time and take tax adjustment.

r) GST (if applicable) on account of liquidated damages due to delay in supply would be borne by DSA.

s) The place of supply under GST Act shall be the place of supply as determined under purchase order raised by BSNL.

t) DSA agrees to share the monthly information with BSNL which would be uploaded by DSA in its GSTR -1 along with the information of input credit to be claimed by BSNL in such month.

13.3.4 Rural Distributor

Rural distributors will cater to rural areas and engagement of these distributors will be through a committee constituted by the SSA Head. The committee will recommend suitable persons/agency from amongst working FMCG distributors/retail shop OR any other suitable person of the area. Based on recommendation of committee, RDs will be selected by the SSA Head.

13.3.4.1 Key features of Rural Distributor Policy

a) Rural distributors may work on non-exclusive basis i.e., they may also sell products of other operators.

b) The territory of Rural Distributor should be designed in such a manner that maximum distance to be served by Rural Distributor is less than 15 km.

c) Rural distributors must be residents of one of the villages of the area which they are serving so that they have good knowledge of local conditions and local market. They are able to push the product deep into the market due to their personal relations with local people.

d) Rural distributors directly serve the retailers and they do not have any employee(s). They will primarily be served by existing franchisee of that area. In case, the franchisee fails to serve, the RD will be served by BSNL directly.

e) Retailer/POS in the area of RD will be managed by Rural Distributors and franchisee will have no direct role to play in that area.

13.3.4.2 Service to Rural Distributor (RDs)

a) RDs will be served by the Territory Franchisee at his doorstep.

b) If Territory Franchisee does not serve the RDs properly then RDs will be served by BSNL directly.

c) Territory Franchisee will collect all CAFs from RDs and will provide them SIM as well as Recharge Coupon/C-TOPUP.

d) RDs will make payment at the time of delivery of stock. Representative of Territory Franchisee will deliver the stock at their doorstep.

e) Suitable unlimited Broadband plan will be given to willing RD free of cost.

13.3.4.3 Responsibilities of Rural distributor:

It is the responsibility of RDs to generate demand for providing services permitted by BSNL. Selling of all BSNL Products assigned to them, directly or through retailers. Not only the targets set are to be achieved but also efforts are to be made to surpass it.

a)Timely submission of bills and claims to the nodal officer/ franchisee.

b)MIS as per BSNL format to BSNL officials/ Franchisee as per frequency specified.

c)Rural Distributor must ensure that BSNL products are available in retail networks in sufficient quantity on demand.

d)Verification of credentials of customers .

e)Rural distributors will be responsible for all the work done through retailers.

f)Rural distributors are required to attend meetings in SSA/ Franchisee as and when needed. Rural Distributor must ensure availability of BSNL products.

13.3.4.4 Responsibilities of BSNL

a) BSNL shall from time to time or in response to specific request by the Rural Distributor provide information, training and assistance relating to the services and arrange for qualified personnel / representatives of BSNL to render such training and assistance.

b) BSNL may provide the marketing material to the Rural distributor.

c) In order to manage returns of defective products, BSNL may, with prior approval of the Rural Distributor, inspect the stock at Rural Distributor‟s location to evaluate whether or not the products are maintained in proper condition.

d) BSNL / its representative will ensure no black marketing happens & also have periodic inspection / surprise check to ensure all channels are working properly.

e) The discounts offered by BSNL are subject to variation during the term of this Agreement at the sole discretion of BSNL.

f) The Rural Distributor can supply the printed / display material etc. at his own cost without any liability on BSNL. He will keep BSNL indemnity from the content of the publicity/ display material so supplied.

13.4 ROLES OF SALES TEAM MEMBER

Roles of different members of the mobility sales team are mentioned below

13.4.1 Roles Of Circle Sales Team:

a) Appointment of franchisees.

b) Monitoring of SSA / Franchisee wise sales and performance w.r.t. target.

c) Ensuring the growth of sales channel network.

d) Ensuring appointment of sales team in SSA.

e) Monitoring the performance of FM/ RMC/ RM.

f) Ensuring the action to be taken by the SSAs.

g) Ensuring the smooth functioning of sales tools such as Sancharsoft, C-TOPUP, B&CCS terminals etc.

h) Redressal of issues / queries reported by the SSAs/ Franchisees.

i) Redressal of cross selling.

j) Escalating the unresolved problems and suggestion to improve the sale to BSNL.

13.4.2 Roles Of SSA Sales Team:

a) Fixing of target for franchisees.

b) Monitoring the sales and performance of sales partner w.r.t. the target on daily / weekly basis.

c) Growth of sales channel network.

d) Appointment of required sales team of FM/ RMC/ RM.

e) Monitoring the performance and visit of FM/ RMC/ RM.

f) Set-up and smooth functioning of sales tools such as Sancharsoft, C-TOPUP, B&CCS terminals etc.

g) Area demarcation and allotment of retailers.

h) Consolidation of priority list of retailers.

i) Support in ordering and delivering of material to sales channel.

j) Ensuring the availability of BSNL product, tariff details, advertising material to all POS.

k) Redressal of cross selling.

l) Payment of allowances / KPA.

m) Redressal of issues / queries reported by Sales partner/ sales channel team.

n) Escalating the unresolved issues and suggestions to improve the sale to Circle office.

13.4.3 Roles Of SSA Franchisee Manager:

a) Communicating target before beginning of month i.e. by 25th of previous month.

b) Support in ordering and delivery of material to Franchisee doorstep.

c) Communication /action raised by the RMCs / RMs.

d) Collection of data from franchisee.

e) Review of franchisee data with SSA sales team.

f) Supply of POS material to franchisee.

g) Ensure proper uses of Sancharsoft and data entry by Franchisee.

h) Redressal of issues / queries of Franchisee.

13.4.4 Roles Of SSA Retail Manager Coordinator (RMC):

a) Plan RM visit to existing retailers and to potential area for appointment of new retailer.

b) Daily review of RM performance.

c) Appointment of new retailers in potential area.

d) Verification of cross selling cases.

e) Compilation of daily report submitted by the RM.

f) Submission of retailer wise data regarding material availability, issues etc to FM with a copy to SSA Sales Head for action.

g) Providing the information regarding BSNL product / schemes / trade schemes/ VAS etc to retailer manager for further publicity.

h) Conduct validation visits with RMs and FMs.

i) Entry of new C-TOPUP retailers‟ information in Sancharsoft.

j) Organization of joint visit of RM and FOS to some distressed retailers.

13.4.5 Roles Of Ssa Retail Manager (RM):

a)Auditing the no. of visits by the FOS to retailers.

b)Auditing the incentives paid to retailers by the Franchisee.

c)Providing the information regarding BSNL product / schemes / trade schemes/ VAS etc to retailer for further publicity.

d)Feedback about replacement of damaged material by the franchisee.

e)Feedback on supply of POS material such as Glow sign board etc.

f)Assessment of potential area for appointment of new retailers.

g)Combined visit with FOS and on spot issuing of C-TOPUP.

13.5 CONCLUSION

Initially BSNL was having one sales channel, that is Customer Care Center (CSC) through which BSNL was selling its product & services. Now as per the changing needs of the customer BSNL has opened up lots off sales Channel like Franchisee, e-Distributor, DSA, Rural Distributor etc. to better serve its customers.

14 PAN TECHNOLOGY OVERVIEW, PAN SWITCHES AND OCPAN

14.1 LEARNING OBJECTIVES

- PAN overview
- PAN switches and OCPAN

14.2 INTRODUCTION: WHAT IS PAN?

Packet Aggregation Network (PAN) is designed to work between access and the core network. PAN switches aggregate voice, video, and data (Any type of traffic STM1, Ethernet, IP, ATM) from the access network and hands it over to the core (IP-MPLS/OTN). PAN equipment has high capacity and works in ring topology to provide protection to the traffic.

PAN is MPLS-TP (Multi Protocol Label switching – Transport Profile) based Converged Packet Aggregation Network Equipment. It is connection oriented.

Transport networks provide transparent transmission of client data traffic between connected client devices by establishing and maintaining point-to-point or point-to-multipoint connections between such devices. The network is basically independent of any higher-layer network that may exist between clients.

In addition to client traffic, a transport network must carry traffic to facilitate its own operation that is necessary for connection control, operation, administration, and maintenance (OAM) functions, network management systems (NMSs), and protection, just as traditional dedicated circuit-based transport technologies such as synchronous digital hierarchy (SDH) and optical transport networks (OTNs), have satisfactory grade capabilities of these functions.

A migration from a legacy network to a new packet transport network is one of the most serious issues for telecom carriers. The development of packet transport network technology has been aimed at achieving functionality similar to that of traditional transport networks achieved by SDH or OTN, which is used to accommodate legacy services including public switched telephone network (PSTN) lines, private leased lines, and clock signal paths.

Thus, the packet transport network must efficiently accommodate IP-oriented services while retaining the existing services by replacing an existing legacy SDH-based transport network. Another issue in deploying a packet transport network is flexibility in introducing emerging new technologies such as software defined networking (SDN) and low cost L3 switch clustering.

14.3 AGGREGATION NETWORK DEPLOYED IN MPLS BASED NETWORK PRIOR TO PAN SWITCHES

It consists of multi-gigabit, Multi-Protocol Label Switching (MPLS) based IP Network in the form of a 2-layered centrally managed IP backbone network designed to provide convergent network supporting data, voice and video applications. The network is envisaged to support the QoS features with four different classes of traffic viz Platinum, Gold, Silver and Bronze along with MPLS- Traffic Engineering, Fast Reroute, multi-casting. This network consists of Core routers (A1, A2, A3 & A4) from different vendors in different locations.

BSNL has deployed a RPR technology based Aggregation Network in the 98 cities for aggregating the Metro IP Traffic. There are around 1200 RPR based switches deployed as Metro Aggregation.

BSNL has also deployed a LAN Switch Based Aggregation Network for aggregating the traffic from the other small cities (OCLAN switches) other than classified RPR based aggregation is deployed.

There are around 3000 LAN switches deployed in the Network for OC City Aggregation (OCLAN)

Typical deployment architecture is given below.

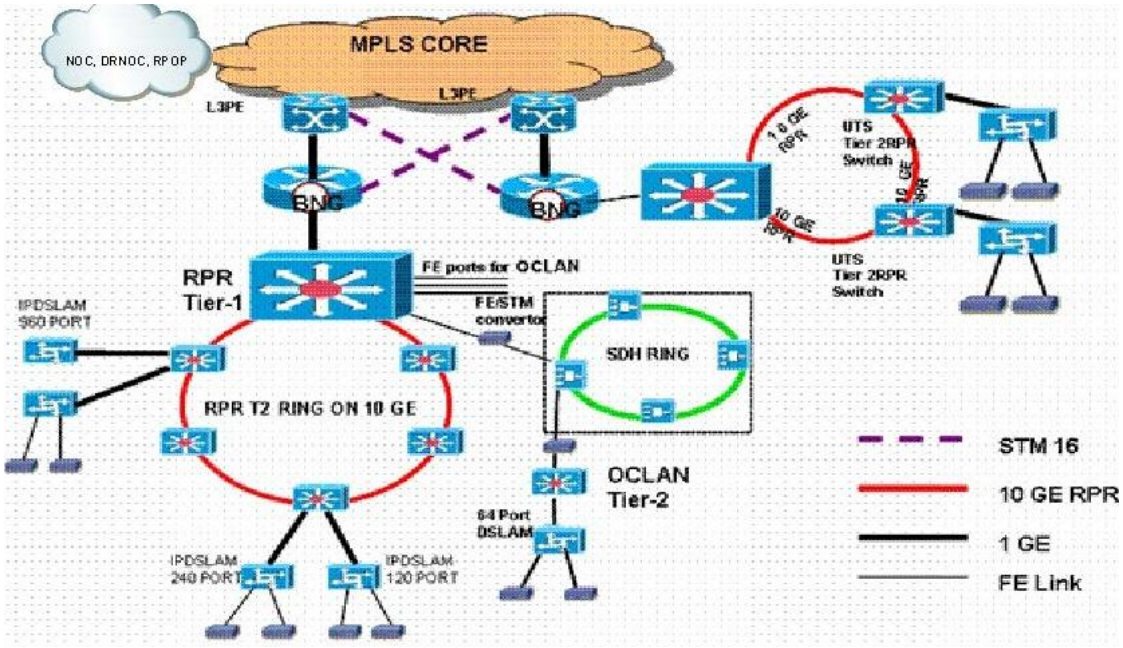


Figure 74: **Broadband Aggregation Network Architecture Prior to PAN Switches**

14.4 FUNCTIONAL REQUIREMENT OF THE PAN SWITCHES & OCPAN

- The PAN switches in the aggregation domain are expected to collect the customer traffic from access network elements like DSLAM, MSAN or FTTH and hand over to the IP-MPLS core network.
- The MNG-PAN shall have functionality like ability to create Ethernet Layer 2 VPN such as point to point, point to multipoint as well as multipoint to multipoint to isolate the customer traffic into their own logical virtual network.
- The switching fabric plane shall be bidirectional and non-blocking. The MNG-PAN Switch shall support a wire speed L2 switching capabilities under full load conditions.
- The MNG-PAN switches shall support built in power diagnostics to monitor optical SFP/XFP ports, system diagnostics hardware failures.
- The equipment shall be Carrier Class with a modular chassis design. By Carrier class, it is implied that the chassis shall have high availability and redundancy features, rack mountable and support easy expansion through addition of tributary cards within the same chassis.
- The aggregation switch shall be architecturally designed such that there is no single point of failure. For this, the architecture shall provide 'packet switching fabric' redundancy.
- The resiliency of the equipment shall be sub 50msec recovery in Ethernet rings for aggregation layer.
- The solution shall interface to the existing BNG and nationwide MPLS core network wherever required.
- The MNG-PAN switches shall support point to point, point to multipoint and multipoint to multipoint traffic in full duplex mode of working.
- The MNG-Pan switches shall be able to function in terminal mode, hub, mesh, and ring topology.
- The MNG-PAN switches shall provide managed multi-service integration viz voice, video, and data.

14.5 DEPLOYMENT ARCHITECTURE OF PAN SWITCHES

BSNL deployed MNG-PAN Aggregation Network in the 15 cities

- 421 PAN-COAU & PAN
- 287 OC PAN

The deployment of the MNG-PAN switch in the network shall be as below:

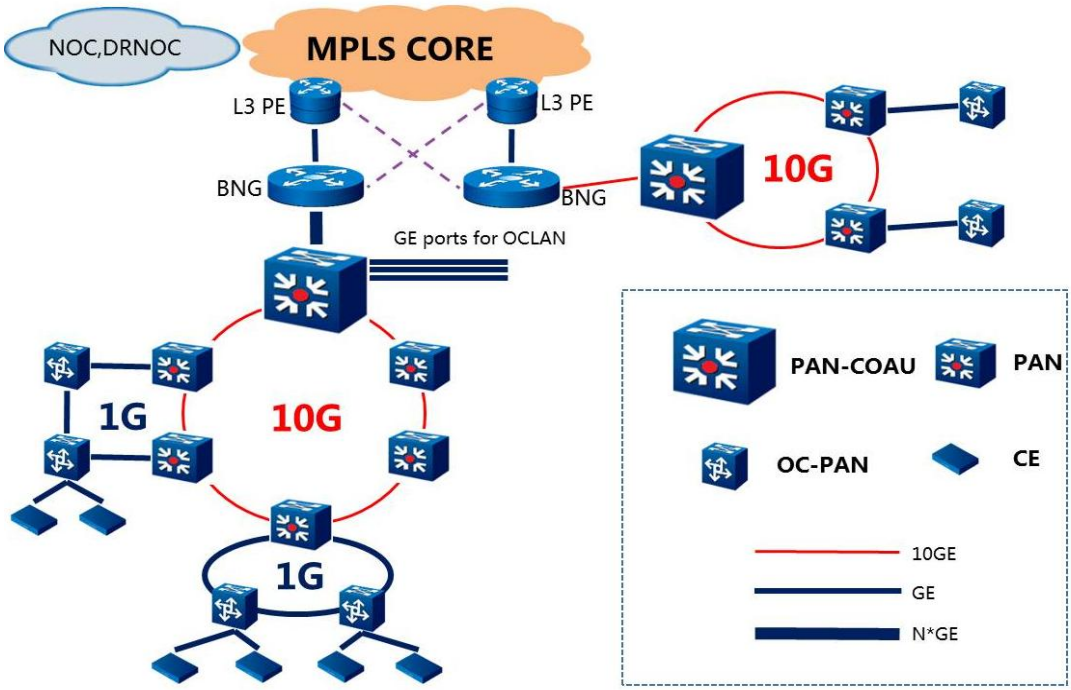


Figure 75: **Deployment Architecture of PAN Switches and OC-PAN**

***PAN – COAU: Packet Aggregation Network – Central Office Aggregation Unit switch: for connecting to BNG or to MPLS routers*

**OC-PAN – Other City Packet Aggregation Network switch*

The OC-PAN ring will aggregate the traffic from all nodes and hand over the traffic to the upper MNG-PAN ring. The Central Office Aggregation Unit (COAU) switch of the PAN ring will aggregate the traffic from all the PAN nodes and hand over the traffic to the IP-MPLS core.

The network shall support internetworking between the MPLS-TP and IP/MPLS domains by any of the solutions

- MPLS-TP Termination - service termination at the edge of each domain and traffic hand over UNI.
- MPLS-TP is a carried over IP-MPLS: service /Tunnel not terminated at the hand-off point, hand-off to core over S-VLAN tunnels or using GRE tunnels
- The equipment shall support the bridging functionality between MPLS-TP and IP/MPLS domains.

14.6 FEATURES OF PAN NETWORK

1. The solution is based on Pseudo Wire over MPLS-TP technology that supports an efficient Ethernet aggregation.

2. The PAN platform offers wide range of protocols, standards and interfaces coupled with highest reliability

3. Carrier-class set of features, including the carrier class sub 50ms recovery resiliency,
4. Hard QoS/SLA guarantees,
5. End to end and multi-layer OAM, network-wide time/clock synchronization,
6. Efficient multicast data distribution.
7. Range of interfaces up to 10GE
8. Low power consumption
9. Centralized management

14.7 ADVANTAGES OF PAN TRANSPORT NETWORK

Scalability: Support of electrical and optical Ethernet interfaces from FE to 10GE. Large switching capacity.

Reliability: Carrier class reliability with fully redundant hardware architecture.

Resilience: Various protection schemes, sub-50ms failure recovery.

Manageability: Enhanced OAM capability with end-to-end service management. NMS-based operation.

Inter-operability: Compliant with ITU-T MPLS-TP standard. Easy integration with core IP/MPLS or OTN networks.

Bandwidth Efficiency: Packet nature of the network with flexible data-pipes enables users to request the service in smaller increments and provides better utilization at the aggregation level.

Lower TCO: Low power consumption; bandwidth efficiency due to optimized packet aggregation; fast f**ault isolation and simple management; smaller form factor.**

14.8 PAN SWITCHES AND OCPAN

PAN switches deployed for MNG-PAN of M/s FiberHome are as given below:

- PAN-COAU : CiTRANS 660
- PAN : CiTRANS 660
- OC-PAN : CiTRANS 650

PAN network is used to replace the existing RPR aggregation network

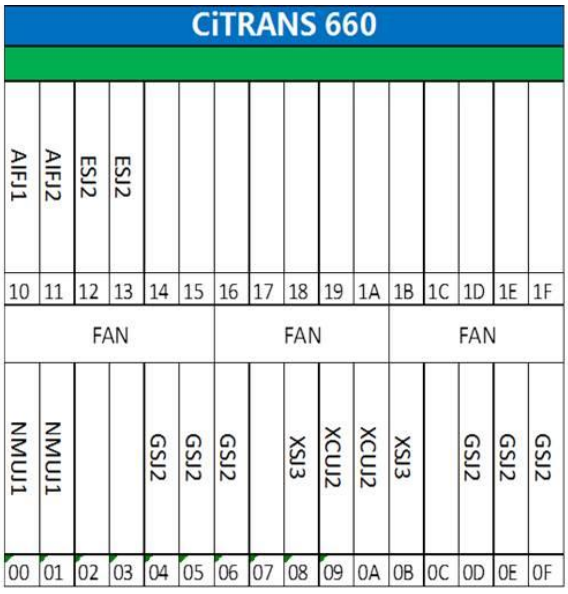
- T1 switches by PAN COAU (CiTRANS 660)
- T2 switches by PAN switch (CiTRANS 660)
- OC-LAN switches by OC PAN (CiTRANS 650 U3)

14.8.1 Pan Coau & Pan Switch (Citrans 660)

Max interface capability

Switch capacity	Interface type				
	10GE	GE	FE	STM-1	E1
160 Gbps	14	120	168	120	224
320 Gbps	30	140	168	128	224

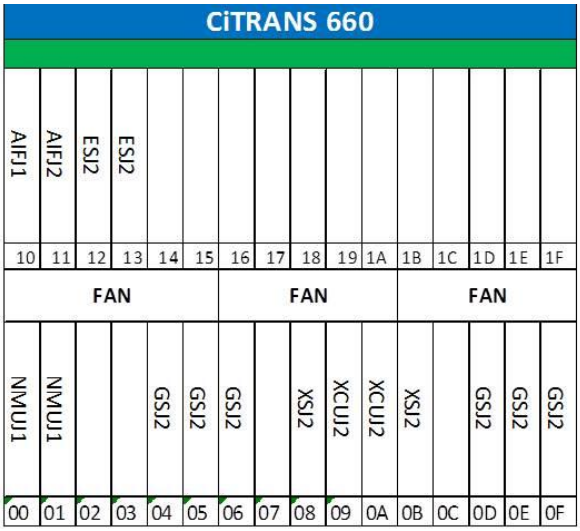
a. COAU-PAN



Abbr.	Card Description
XCUJ2	Cross Connection & Clock Unit (320G)
NMUJ1	Network Management Unit
AIFJ1	Power & Auxiliary Panel1
AIFJ2	Power & Auxiliary Panel2
XSJ3	10G LAN/WAN Optical Card (4 ports)
GSJ2	GE Optical Card (10 ports)
ESJ2	FE Optical Card (12 ports)

Power Consumption: 625 Watt

b. PAN



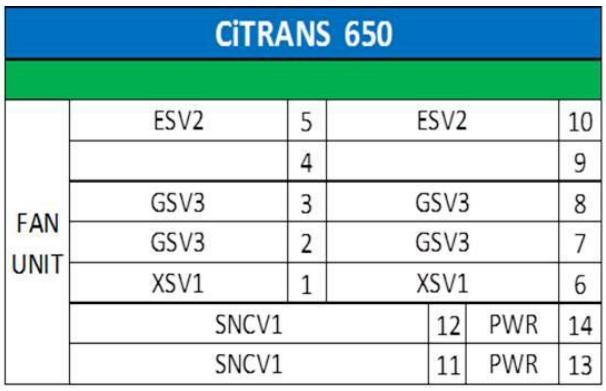
Abbr.	Card Description
XCUJ2	Cross Connection & Clock Unit (320G)
NMUJ1	Network Management Unit
AIFJ1	Power & Auxiliary Panel1
AIFJ2	Power & Auxiliary Panel2
XSJ2	10G LAN/WAN Optical Card (2 ports)
GSJ2	GE Optical Card (10 ports)
ESJ2	FE Optical Card (12 ports)

Power Consumption: 535 Watt

2. OC-PAN

Max interface capability

Interface type				
10GE	GE	FE	STM-1	E1
10	80	80	40	320



Abbr.	Card Description
SNCV1	Cross Connection & EMU (100G)
PWR	Power Card
XSV1	10G LAN/WAN Optical Card (1 ports)
GSV3	GE Optical Card (8 ports)
ESV2	FE Optical Card (8 ports)

Power Consumption: 408 Watt

14.9 CONCLUSION

The PAN and OC-PAN switches shall collect the customer traffic like voice, video and data being generated through different access Broadband networks such as DSL, FTTH, MSAN, 3G Node B, Wi-Max etc and hand over to IP-MPLS core network.

15 OVERVIEW OF OPTICAL COMMUNICATION

15.1 LEARNING OBJECTIVES

- Fiber-Optic Applications
- Basic optical fiber communication system:
- The Structure of an Optical Fiber
- Principle of Operation

15.2 INTRODUCTION

The use of light for transmitting information from one place to another place is a very old technique. In 800 BC., the Greeks used fire and smoke signals for sending information like victory in a war, alerting against enemy, call for help, etc. Mostly only one type of signal was conveyed. During the second century B.C. optical signals were encoded using signaling lamps so that any message could be sent. There was no development in optical communication till the end of the 18th century. The speed of the optical communication link was limited due to the requirement of line of sight transmission paths, the human eye as the receiver and unreliable nature of transmission paths affected by atmospheric effects such as fog and rain.

In the late 19th and early 20th centuries, light was guided through bent glass rods to illuminate body cavities. Alexander Graham Bell invented a 'Photophone' to transmit voice signals over an optical beam. By 1964, a critical and theoretical specification was identified by Dr. Charles K. Kao for long-range communication devices, the 10 or 20 dB of light loss per kilometer standard. Dr. Kao also illustrated the need for a purer form of glass to help reduce light loss. By 1970 Corning Glass invented fiber-optic wire or "optical waveguide fibers" which was capable of carrying 65,000 times more information than copper wire, through which information carried by a pattern of light waves could be decoded at a destination even a thousand miles away. Corning Glass developed fiber with loss of 17 dB/ km at 633 nm by doping titanium into the fiber core. By June of 1972, multimode germanium-doped fiber had developed with a loss of 4 dB per kilometer and much greater strength than titanium-doped fiber.

In April 1977, General Telephone and Electronics tested and deployed the world's first live telephone traffic through a fiber-optic system running at 6 Mbps, in Long Beach, California. They were soon followed by Bell in May 1977, with an optical telephone communication system installed in the downtown Chicago area, covering a distance of 1.5 miles (2.4 kilometers). Each optical-fiber pair carried the equivalent of 672 voice

channels. Today more than 80 percent of the world's long-distance voice and data traffic is carried over optical-fiber cables.

An **optical fiber** is a thin, flexible, transparent fiber that acts as a waveguide, or "light pipe", to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communications, which permits transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference.

With increase in population struggle for survival increased Its impacts on appearing in human life in many ways. There have been shortage of utilizes resources. The resources consist of materials, technology, money, human recourse, information, interconnectivity etc.

Due to consistent pressure there has been different ways of innovations in almost every stream of life. In the field of telecommunication also development are happening in the fields of client terminals access technique, aggregation technique, multiplexing technique, transport technique. There has been different access technique and different type of client terminals as per respective access technique. The basic contents were limitations of transmission media and low order multiplexing and switching. The initial transmission started with attaching information leaflet with visions. The same concept was utilized on building semaphore. That came the evolution telegraphs lines after the invention of more score in which use of guided media has got important. In this era use of open wire communications having overhead line with minimal multiplexing was the latest things. However has the requirement of reliable telecommunication has increased need was well to have proper voice communications and switching like manual, electro mechanical, fully digital involving automatic increasing order of multiplexing were implemented. In this era the main access network comprised of cable network made up of copper and transmission network was predominately of over head lines. Later on seeing the limitations of over head lines like deterioration weather due to electro magnetite interference less carrying capacity ete. were found. Use of optical fibre as a transmission media got thrust due to less cost, improve technology in multiplexing, virtually infants capacity and immunity to electro-magnetic interference. Requirement of bandwidth which was around 20Kbps have reached to around 1Gbps. The accesses network is also converging with the development of IP & MPLS technologies of dada communication. Multiplexing is also migrating in TDM, FDM to packet base statistical multiplexing. Client terminals are also converging having all capabilities of voice, video, text, web and multimedia. The network is converging to one by using architecture of Next Generation network. Applications which were accesses network depended are also becoming universally accessible and a accesses network agnostic. The human interface is also improve presentably because of manufacturing line terminal incorporating signals of

sensory organs like touch, vision, mind etc.. Today client terminals have improve GUI based web interface having faster processing multimedia capacity and capability to communicate to multiple secessions over multiple windows having full mobility as well as portability.

Due to competitions and rapid growth of innovation, the world are become faster and expectations of prominent service delivery are also been increased. Delay in providing services has also been reduced and overall connectivity in becoming P-P i.e. pair to pair.

15.3 FIBER-OPTIC APPLICATIONS

The use and demand for optical fiber has grown tremendously and optical-fiber applications are numerous. Telecommunication applications are widespread, ranging from global networks to desktop computers. These involve the transmission of voice, data, or video over distances of less than a meter to hundreds of kilometers, using one of a few standard fiber designs in one of several cable designs.

- Long distance communication backbones
- Inter-exchange junctions
- Video transmission
- Broadband services
- Computer data communication (LAN, WAN etc.)
- High EMI areas
- Non-communication applications (sensors etc…)

15.4 ADVANTAGES OF OPTICAL FIBER COMMUNICATION

Fiber Optics has the following advantages:

Wider bandwidth: The information carrying capacity of a transmission system is directly proportional to the carrier frequency of the transmitted signals. The optical carrier frequency is in the range 10^{13} to 10^{15} Hz while the radio wave frequency is about 10^{6} Hz and the microwave frequency is about 10^{10} Hz. Thus the optical fiber yields greater transmission bandwidth than the conventional communication systems and the data rate or number of bits per second is increased to a greater extent in the optical fiber communication system. Further the wavelength division multiplexing operation by the data rate or information carrying capacity of optical fibers is enhanced to many orders of magnitude.

Low transmission loss: Due to the usage of the ultra low loss fibers and the erbium doped silica fibers as optical amplifiers, one can achieve almost lossless transmission. In the modern optical fiber telecommunication systems, the fibers having a transmission loss of 0.2dB/km are used. Further, using erbium doped silica fibers over a short length in the

transmission path at selective points; appropriate optical amplification can be achieved. Thus the repeater spacing is more than 100 km. Since the amplification is done in the optical domain itself, the distortion produced during the strengthening of the signal is almost negligible.

Dielectric waveguide: Optical fibers are made from silica which is an electrical insulator. Therefore they do not pickup any electromagnetic wave or any high current lightning. It is also suitable in explosive environments. Further the optical fibers are not affected by any interference originating from power cables, railway power lines and radio waves. There is no cross talk between the fibers even though there are so many fibers in a cable because of the absence of optical interference between the fibers.

Signal security: The transmitted signal through the fibers does not radiate. Further the signal cannot be tapped from a fiber in an easy manner. Therefore optical fiber communication provides hundred per cent signal security.

Small size and weight: Fiber optic cables are developed with small radii, and they are flexible, compact and lightweight. The fiber cables can be bent or twisted without damage. Further, the optical fiber cables are superior to the copper cables in terms of storage, handling, installation and transportation, maintaining comparable strength and durability.

15.5 FIBER OPTICS BASICS: PRINCIPLES OF OPTICAL COMMUNICATION

Optical Fiber is new medium, in which information (voice, Data or Video) is transmitted through a glass or plastic fiber, in the form of light, following the transmission sequence give below:

(1) Information is encoded into Electrical Signals.

(2) Electrical Signals are converted into light Signals.

(3) Light Travels down the Fiber.

(4) A Detector Changes the Light Signals into Electrical Signals.

(5) Electrical Signals are decoded into Information.

- Inexpensive light sources available.

- Repeater spacing increases along with operating speeds because low loss fibres are used at high data rates.

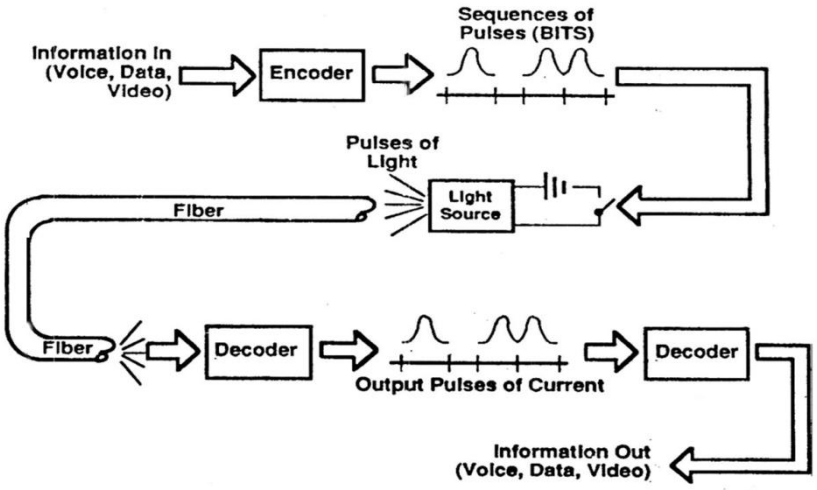


Figure 76: **Fiber Optic System**

15.6 PRINCIPLE OF OPERATION - THEORY

Speed of light is actually the velocity of electromagnetic energy in vacuum such as space. Light travels at slower velocities in other materials such as glass. Light travelling from one material to another changes speed, which results in changing its direction of travel. This deflection of light is called Refraction. The amount that a ray of light passing from a lower refractive index to a higher one, is bent towards the normal, but light going from a higher index to a lower one, refracting away from the normal, as shown in the figures.

The basics of light propagation can be discussed with the use of geometric optics. The basic law of light guidance is Snell's law (Fig. 77). Consider two dielectric media with different refractive indices and with n1 >n2 and that are in perfect contact, as shown in Figure. At the interface between the two dielectrics, the incident and refracted rays satisfy Snell's law of refraction—that is,

$n1\sin\varphi1 = n2\sin\varphi2$

In addition to the refracted ray there is a small amount of reflected light in the medium with refractive index n1. Because n1 is greater than n2 then always **$\phi2 > \phi1$**. As the angle of the incident ray increases there is an angle at which the refracted ray emerges parallel to the interface between the two dielectrics. This angle is referred to as the critical angle, ϕcrit, and from Snell's law is given by

$\sin\varphi crit = n2/n1$

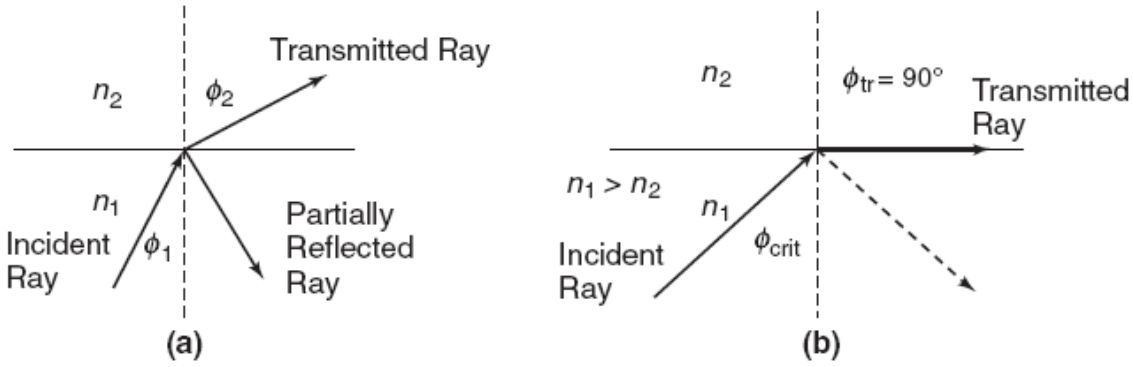


Figure 77: **Snell's law**

If the angle of incidence increases amore than the critical angle, the light is totally reflected back into the first material so that it does not enter the second material. The angle of incidence and reflection are equal and it is called **Total Internal Reflection**.

15.6.1 Propagation Of Light Through Fibre

The optical fiber has two concentric layers called the core and the cladding. The inner core is the light carrying part. The surrounding cladding provides the difference refractive index that allows total internal reflection of light through the core. The index of the cladding is approximately 1% lower than that of the core. Typical values for example are a core refractive index of 1.47 and a cladding index of 1.46. Fiber manufacturers control this difference to obtain desired optical fiber characteristics. Most fibers have an additional coating around the cladding. This buffer coating is a shock absorber and has no optical properties affecting the propagation of light within the fiber. Figure shows the idea of light travelling through a fiber. Light injected into the fiber and striking core to cladding interface at greater than the critical angle, reflects back into core, since the angle of incidence and reflection are equal, the reflected light will again be reflected. The light will continue zigzagging down the length of the fiber. Light striking the interface at less than the critical angle passes into the cladding, where it is lost over distance. The cladding is usually inefficient as a light carrier, and light in the cladding becomes attenuated fairly. Propagation of light through fiber is governed by the indices of the core and cladding by Snell's law.

Such total internal reflection forms the basis of light propagation through a optical fiber. This analysis consider only meridional rays- those that pass through the fiber axis each time, they are reflected. Other rays called Skew rays travel down the fiber without passing through the axis. The path of a skew ray is typically helical wrapping around and around the central axis. Fortunately skew rays are ignored in most fiber optics analysis.

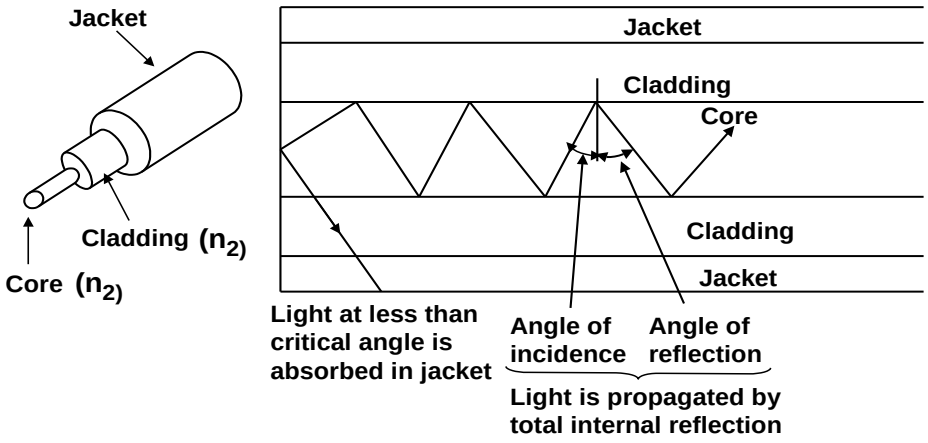


Figure 78: **Propagation of light through fiber**

The specific characteristics of light propagation through a fiber depends on many factors, including

- The size of the fiber.
- The composition of the fiber.

The light injected into the fiber

15.6.2 Geometry Of Fiber

The optical fibers used in communications have a very simple structure. A hair-thin fiber consist of two concentric layers of high-purity silica glass the core and the cladding, which are enclosed by a protective sheath as shown in Figure. Core and cladding have different refractive indices, with the core having a refractive index, n1, which is slightly higher than that of the cladding, n2. It is this difference in refractive indices that enables the fiber to guide the light. Because of this guiding property, the fiber is also referred to as an "optical waveguide." As a minimum there is also a further layer known as the secondary cladding that does not participate in the propagation but gives the fiber a minimum level of protection, this second layer is referred to as a coating. Light rays modulated into digital pulses with a laser or a light-emitting diode moves along the core without penetrating the cladding.

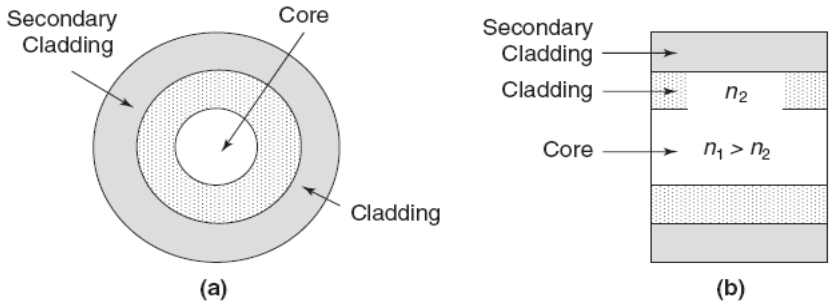


Figure 79: **(a) Cross section and (b) longitudinal cross section of a typical optical fiber**

The light stays confined to the core because the cladding has a lower refractive index—a measure of its ability to bend light. Refinements in optical fibers, along with the development of new lasers and diodes, may one day allow commercial fiber-optic networks to carry trillions of bits of data per second.

The light stays confined to the core because the cladding has a lower refractive index—a measure of its ability to bend light. Refinements in optical fibers, along with the development of new lasers and diodes, may one day allow commercial fiber-optic networks to carry trillions of bits of data per second.

The diameters of the core and cladding are as follows.

Core (μm)	**Cladding (μm)**
8	125
50	125
62.5	125
100	140

Fibre sizes are usually expressed by first giving the core size followed by the cladding size. Thus 50/125 means a core diameter of 50μm and a cladding diameter of 125μm.

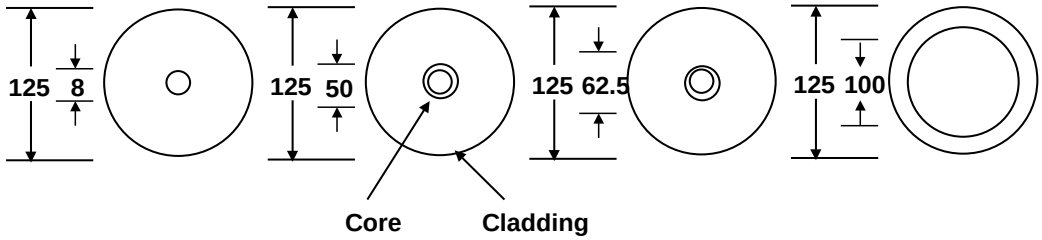


Figure 80: **Typical Core and Cladding Diameter**

15.7 FIBRE TYPES – SINGLE MODE AND MULTI-MODE

The refractive Index profile describes the relation between the indices of the core and cladding. Two main relationships exist:

(I) Step Index

(II) Graded Index

The step index fibre has a core with uniform index throughout. The profile shows a sharp step at the junction of the core and cladding. In contrast, the graded index has a non-uniform core. The Index is highest at the center and gradually decreases until it matches with that of the cladding. There is no sharp break in indices between the core and the cladding.

By this classification there are three types of fibres :

(I) Multimode Step Index fibre (Step Index fibre)

(II) Multimode graded Index fibre (Graded Index fibre)

(III) Single- Mode Step Index fibre (Single Mode Fibre)

15.7.1 Step-Index Multimode Fiber

Step Index multimode Fiber has a large core, up to 100 microns in diameter. As a result, some of the light rays that make up the digital pulse may travel a direct route, whereas others zigzag as they bounce off the cladding. These alternative pathways cause the different groupings of light rays, referred to as modes, to arrive separately at a receiving point. The pulse, an aggregate of different modes, begins to spread out, losing its well-defined shape. The need to leave spacing between pulses to prevent overlapping limits bandwidth that is, the amount of information that can be sent. Consequently, this type of fiber is best suited for transmission over short distances, in an endoscope, for instance.

Figure 81: **STEP-INDEX MULTIMODE FIBER**

15.7.2 Graded-Index Multimode Fiber

It contains a core in which the refractive index diminishes gradually from the center axis out toward the cladding. The higher refractive index at the center makes the light rays moving down the axis advance more slowly than those near the cladding.

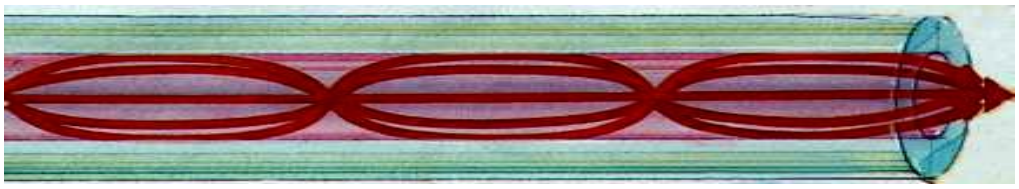


Figure 82: **GRADED-INDEX MULTIMODE FIBER**

Also, rather than zigzagging off the cladding, light in the core curves helically because of the graded index, reducing its travel distance. The shortened path and the higher speed allow light at the periphery to arrive at a receiver at about the same time as the slow but straight rays in the core axis. The result: a digital pulse suffers less dispersion.

15.7.3 Single-Mode Fiber

It has a narrow core (nine microns or less), and the index of refraction between the core and the cladding changes less than it does for multimode fibers. Light thus travels parallel to the axis, creating little pulse dispersion. Telephone and cable television networks install millions of kilometers of this fiber every year.

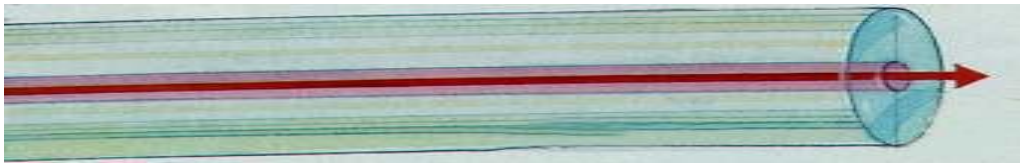


Figure 83: **SINGLE-MODE FIBER**

15.8 CABLE CONSTRUCTION

There are two basic cable designs are:

1. Tight Buffer Tube Cable
2. Loose Buffer Tube Cable

Loose-tube cable is used in the majority of outside-plant installations and tight-buffered cable, primarily used inside buildings.

15.8.1 Tight Buffer Tube Cable

With tight-buffered cable designs, the buffering material is in direct contact with the fiber. This design is suited for "jumper cables" which connect outside plant cables to terminal equipment, and also for linking various devices in a premises network. Single-fiber tight-buffered cables are used as pigtails, patch cords and jumpers to terminate loose-tube cables directly into opto-electronic transmitters, receivers and other active and passive components. Multi-fiber tight-buffered cables also are available and are used primarily for alternative routing and handling flexibility and ease within buildings. The tight-buffered design provides a rugged cable structure to protect individual fibers during handling, routing and connectorization. Yarn strength members keep the tensile load away from the fiber.

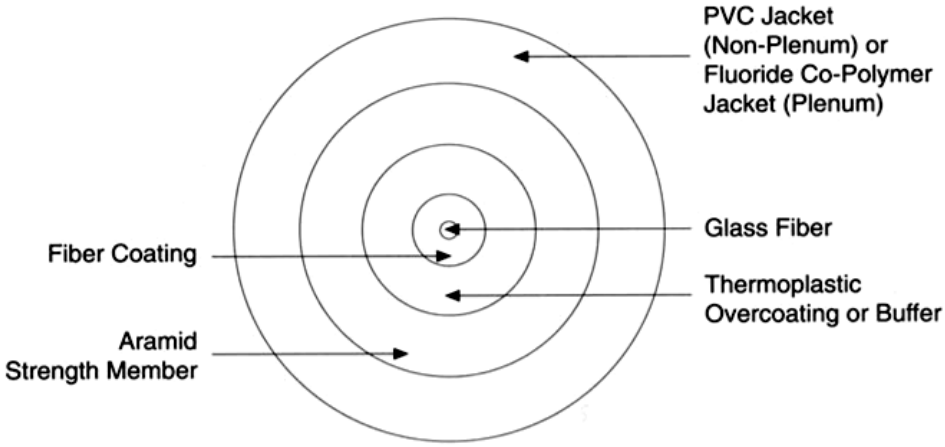


Figure 84: **Tight Buffer Tube Cable**

The structure of a 250um coated fiber (bare fiber)

- Core (9um for standard single mode fibers, 50um or 62.5um for multimode fibers)
- Cladding (125um)
- Coating (soft plastic, 250um is the most popular, sometimes 400um is also used)

15.8.2 Loose-Tube Cable

The modular design of loose-tube cables typically holds **6, 12, 24, 48, 96 or even more than 400 fibers per cable**. Loose-tube cables can be all-dielectric or optionally armored. The loose-tube design also helps in the identification and administration of fibers in the system.

In a loose-tube cable design, color-coded plastic buffer tubes house and protect optical fibers. A gel filling compound impedes water penetration. Excess fiber length (relative to buffer tube length) insulates fibers from stresses of installation and environmental loading. Buffer tubes are stranded around a dielectric or steel central member, which serves as an anti-buckling element.

The cable core, typically uses aramid yarn, as the primary tensile strength member. The outer polyethylene jacket is extruded over the core. If armoring is required, a corrugated steel tape is formed around a single jacketed cable with an additional jacket extruded over the armor. Loose-tube cables typically are used for outside-plant installation in aerial, duct and direct-buried applications.

Loose tube cable is designed to endure outside temperatures and high moisture conditions. The fibers are loosely packaged in gel filled buffer tubes to repel water.

Recommended for use between buildings that are unprotected from outside elements. Loose tube cable is restricted from inside building use.

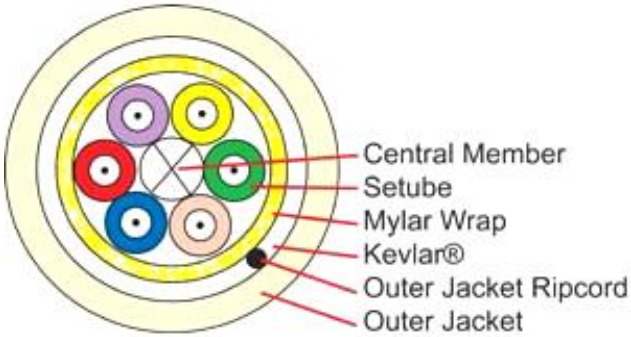


Figure 85: **Loose Tube Cable**

15.8.3 Elements In A Loose Tube Fiber Optic Cable:

1. Multiple 250um coated bare fibers (in loose tube)
2. One or more loose tubes holding 250um bare fibers. Loose tubes strand around the central strength member.
3. Moisture blocking gel in each loose tube for water blocking and protection of 250um fibers
4. Central strength member (in the center of the cable and is stranded around by loose tubes)
5. Aramid Yarn as strength member
6. Ripcord (for easy removal of inner jacket)
7. Outer jacket (Polyethylene is most common for outdoor cables because of its moisture resistant, abrasion resistant and stable over wide temperature range characteristics.)

15.9 TYPES OF FIBER OPTIC CABLE (MOST POPULAR FIBER OPTIC CABLE TYPES)

15.9.1 Indoor Cables

Simplex Fiber Cables

A single cable structure with a single fiber. Simplex cable varieties include 1.6mm & 3mm jacket sizes.

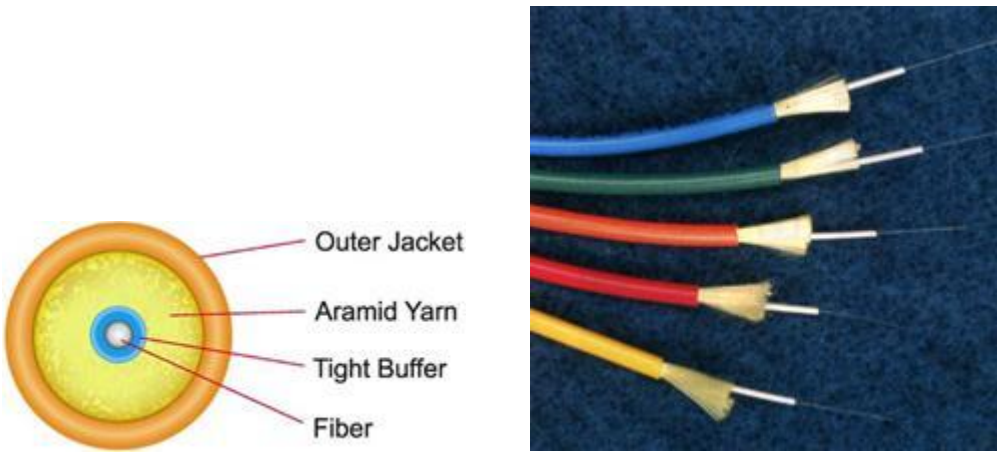


Figure 86: **Simplex Fiber Cables**

Duplex Fiber Optic Cable

This cable contains two optical fibers in a single cable structure. Light is not coupled between the two fibers; typically one fiber is used to transmit signals in one direction and the other receives.

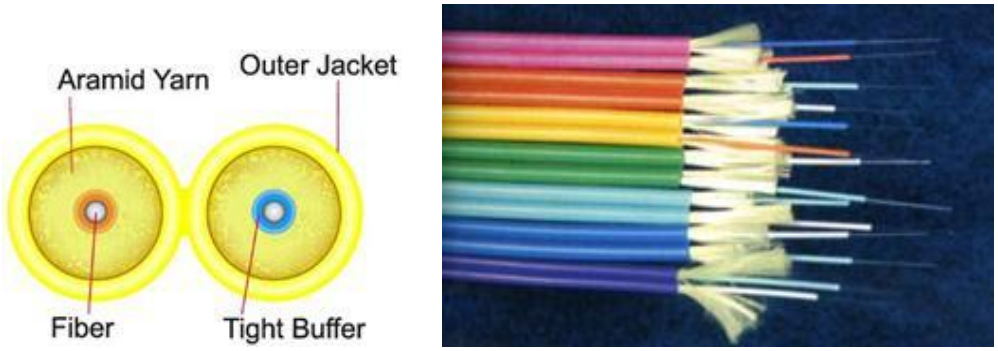


Figure 87: **Duplex Fiber Optic Cable**

15.9.2 Outdoor Loose Tube Fiber Optic Cables

Tube encloses multiple coated fibers that are surrounded by a gel compound that protects the cable from moisture in outside environments. Cable is restricted from indoor use, typically allowing entry not to exceed 50 feet.

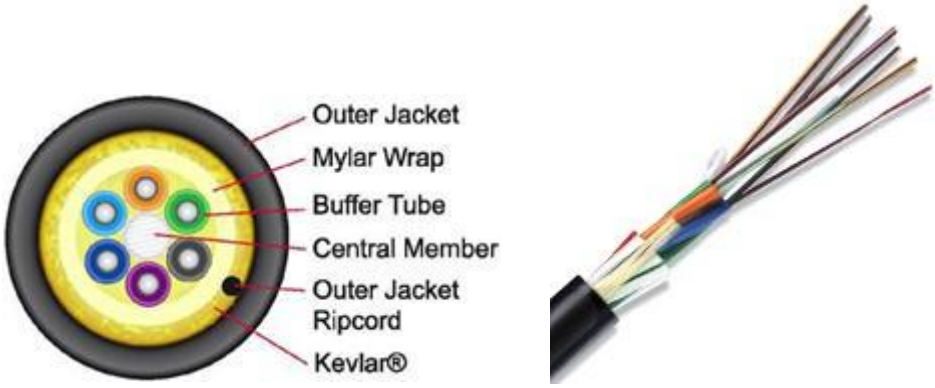


Figure 88: **Outdoor Loose Tube Fiber Optic Cables**

15.9.3 Aerial/Self-Supporting

Figure 97 (aerial/self-supporting) fiber cables are designed to be strung from poles outdoors and most can also be installed in underground ducts. They have internal stress members of steel of steel or aramid yarn that protect fibers from stress.

Aerial cable provides ease of installation and reduces time and cost. Figure 8 cable can easily be separated between the fiber and the messenger. Temperature range -55 to +85°C.

Figure 89: **Aerial cable**

15.9.4 Direct-Buried Armored Fiber Optic Cable

Armored cables are similar to outdoor cables but include an outer armor layer for mechanical protection and to prevent damage. They can be installed in ducts or aerially, or directly buried underground. Armor is surrounded by a polyethylene jacket.

Armored cable can be used for rodent protection in direct burial if required. This cable is non-gel filled and can also be used in aerial applications. The armor can be removed leaving the inner cable suitable for any indoor/outdoor use. Temperature rating -40 to +85°C.

Figure 90: **Armored cable**

15.9.5 Submarine Fiber Optic Cable (Undersea Fiber Optic Cable)

Submarine cables are used in fresh or salt water. To protect them from damage by fishing trawlers and boat anchors they have elaborately designed structures and armors. Long distance submarine cables are especially complex designed.

Figure 91: **Submarine cables**

15.9.6 ITU-T Complaint Fibers

- G.651 Multimode Fiber
- G.652 Standard Fiber
- G.653 Dispersion Shifted Fiber
- G.654 Loss minimized Fiber
- G.655 Non Zero Dispersion Shifted Fiber
- G.656 Medium Dispersion Fiber (MDF), designed for local access
- G.657 Bending Loss Insensitive Fiber

15.10 CHARACTERISTICS OF OPTICAL FIBER

15.10.1 Wavelength

It is a characteristic of light that is emitted from the light source and is measures in nanometers (nm). In the visible spectrum, wavelength can be described as the colour of the light.

For example, Red Light has longer wavelength than Blue Light, Typical wavelength for fibre use are 850nm, 1300nm and 1550nm all of which are invisible (Infrared).

15.10.2 Windows

A narrow window is defined as the range of wavelengths at which a fibre best operates. Typical windows are given below:

Windows	Operational Wavelength
800nm - 900nm	850nm (Ist Window)
1250nm - 1350nm	1310nm (2nd Window)
1500nm - 1600nm	1550nm (3rd Window)

15.10.3 Attenuation

Attenuation in optical fiber is caused by intrinsic factors, primarily scattering and absorption, and by extrinsic factors, including stress from the manufacturing process, the environment, and physical bending.

The primary factors affecting attenuation in optical fibers are the length of the fiber and the wavelength of the light. Figure shows the loss in decibels per kilometer (dB/km) by wavelength from Rayleigh scattering, intrinsic absorption, and total attenuation.

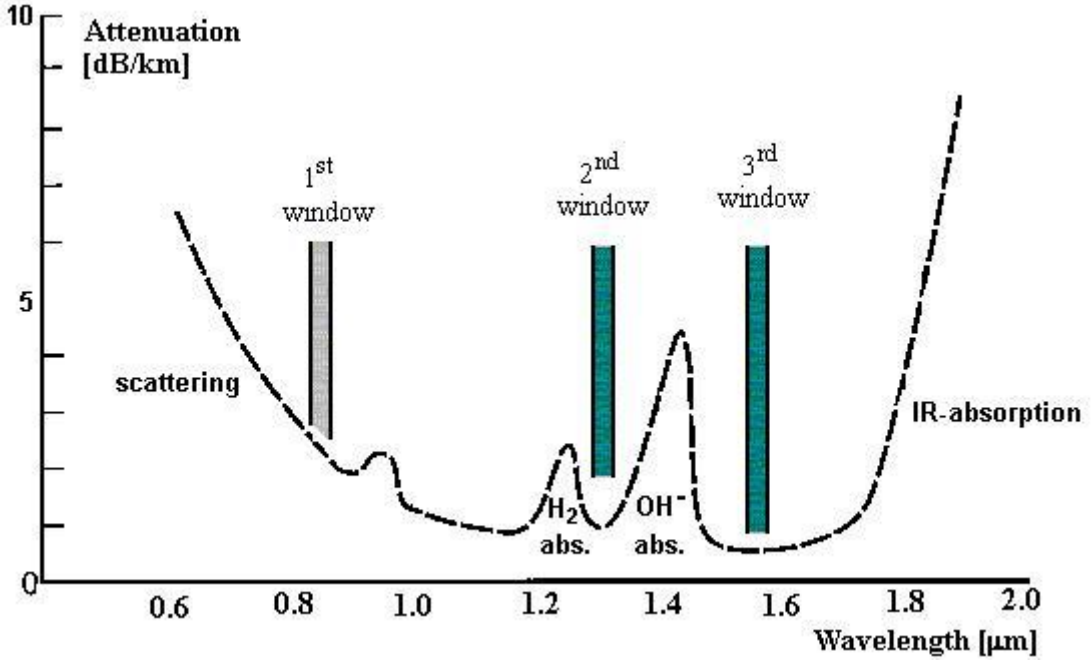


Figure 92: **Attenuation Vs. Wavelength characteristic**

15.10.4 Dispersion

Dispersion is the spreading of light pulse as its travels down the length of an optical fibre as shown in figure The varying delay in arrival time between different components of a signal "smears out" the signal in time. This causes energy overlapping

and limits information capacity of the fiber.

Dispersion limits the bandwidth or information carrying capacity of a fibre. The bit-rates must be low enough to ensure that pulses are farther apart and therefore the greater dispersion can be tolerated.

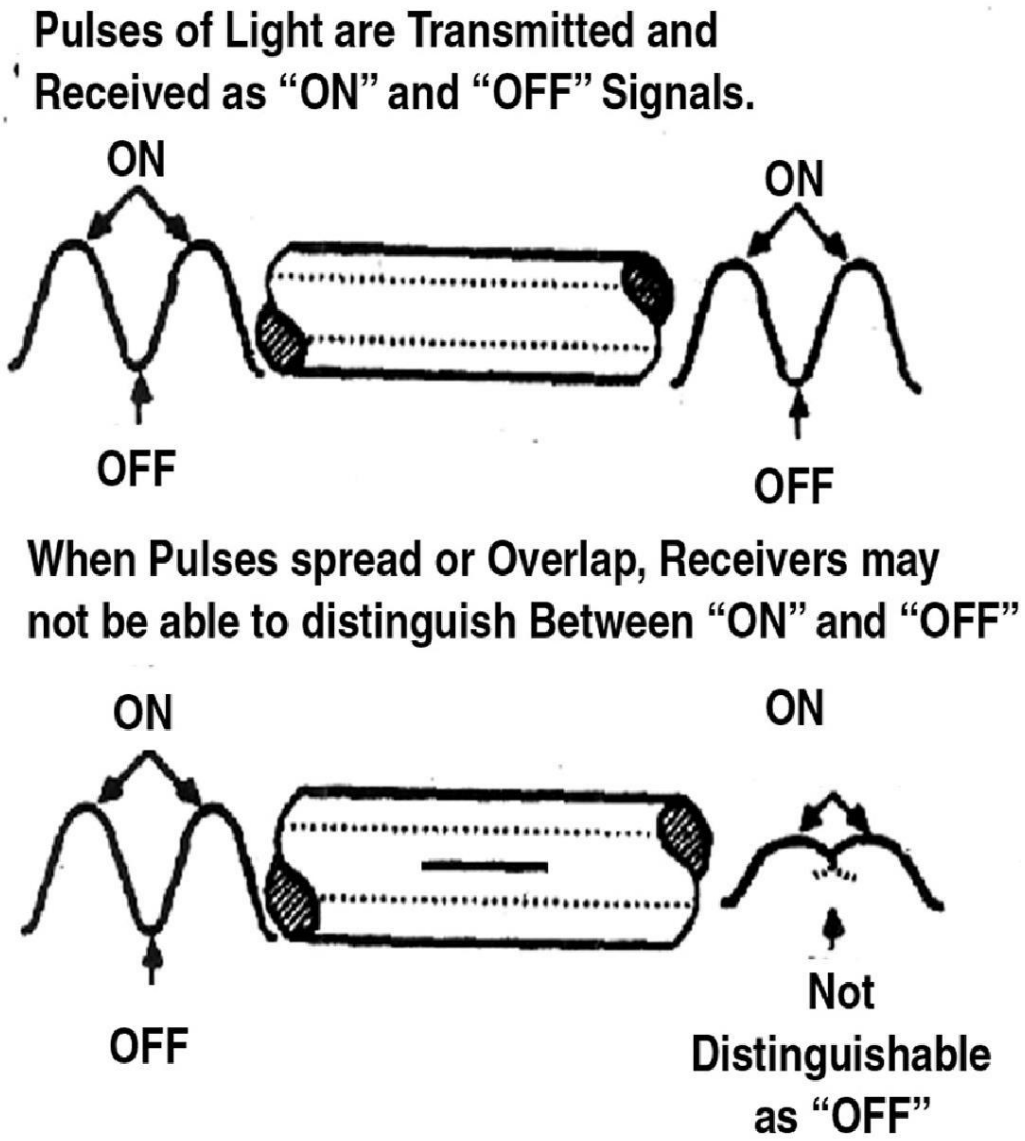


Figure 93: **Dispersion**

15.11 CONCLUSION

Fiber optic technology is a revolutionary technological departure from the traditional copper wires twisted-pair cable or coaxial cable. The usage of optical fiber in the telecommunications industry has grown a few decades ago. Today, many industries particularly telecommunications industry chooses optical fiber over copper wire because of its ability to transmit large amount of information at a time.

An optical fiber is a flexible filament of very clear glass capable of carrying information in the form of light. Optical fibers are hair-thin structures created by forming pre-forms, which are glass rods drawn into fine threads of glass protected by a plastic coating.

16 OVERVIEW OF TRANSPORT NETWORK

16.1 LEARNING OBJECTIVES

- Understand the basics of telecommunication and building blocks of transport network.
- Describe the different types of Transport Network
- Differentiate the different components of transmission network.

16.2 INTRODUCTION

The world today exchanges information in the form of digital voice and data and the transport network is used to carry this information from one place to another. Transport technologies use a media to carry this information. The increase in number of subscribers and the coverage area have mandated an evolution of the transport technologies. Earlier, the information was sent for shorter distances and the operators used copper as a media. The information-carrying capacity of these copper networks was very low. Also, these networks were prone to external disturbances. The fiber optic technology came into picture when the operators felt the need to send more and more voice information for longer distances with less or no external disturbances. In the course of time, subscribers started using more data-driven applications and their demand for bandwidth grew. The earlier networks which were optimized for only voice were proved to be inefficient while carrying video and data traffic. This chapter focuses on the evolution in the transport technology area and describes the OAM functions of transport network and application of the transport network by discussing a case study of mobile backhaul networks.

As a result of the tremendous growth in telecommunications demands during recent decades, much attention has been given to research in the field of telecommunications transport and this has made the telecommunication standard bodies to develop new technologies for transport that are able to carry voice, data and video. Some of these standard bodies and their work are briefed below-

- ITU – ITU's mission is to enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy. ITU is active in the information and communication technology field by defining and adopting the globally agreed technical standards that have allowed industry to interconnect people and equipment seamlessly around the world.

- ETSI - ETSI produces globally-applicable standards for Information and Communications Technologies, including fixed, mobile, radio, converged, broadcast and internet technologies.
- Broadband Forum – The Broadband Forum has defined the core Digital Subscriber Line (DSL) technology and now involved in the delivery of the maximum effectiveness in broadband deployment and use. Best practices for auto-configuration, flow-through provisioning, equipment interoperability and other key facilitators of scalable, global, mass-market deployment of broadband, are developed by the Broadband Forum through a contribution based system and fast-tracked based on service provider market priorities.
- Metro Ethernet Forum - The MEF develops technical specifications and implementation agreements to promote interoperability and deployment of Carrier Ethernet worldwide.

The mission of MEF is to accelerate the worldwide adoption of Carrier-class Ethernet networks and services. Communication service providers nowadays are observing that the major portion of the traffic in their network is dominated by the video and data and not just the voice. Users who extensively use data-oriented applications are now looking to the telecommunication service suppliers to provide the data rates commensurable with those achieved by their own in-house LANs. They also want to be able to transfer information to other metropolitan and international sites as easily and as quickly as they can to a colleague sitting at the next desk. In order to fulfill these requirements of the customers, the operators felt the need of the transport network to be very efficient and flexible. The transport network originally designed to carry only voice traffic should be able to carry voice as well as video and data traffic very efficiently as today's services need bandwidth to support these triple play applications.

16.3 CLASSIFICATION OF TRANSPORT NETWORK BY GEOGRAPHY:-

One traditional approach to classifying transport networks is in relation to their geographic scope. These classifications are illustrated in Figure 102. The access network is that portion of the network that connects the end users (subscribers) to the edge switching elements in the network. The metropolitan (metro) transport network is the network that interconnects central offices (COs) within an urban/suburban region. COs within a metro network are typically directly connected to both access networks and core long distance networks. These metro COs are typically owned by the same carrier, and in many cases either allow the carrier to centralize specialized services (e.g. ISDN or Ethernet routing) in just one CO, or to use different COs for back-up redundancy for each other (e.g., to take over switching functions in the event of a failure of the primary CO for that subscriber). The span lengths between metro COs are typically relatively short. The long distance core transport network provides the interconnection between metro networks, smaller community COs, service providers (e.g., Internet), and regional or international gateways. Higher bandwidth technology typically sees its first deployment

in the core network since the longer facility lengths necessitate more efficient utilization of the facilities. The technology used in the core networks, however, typically eventually finds its way into the metro network as the cost of technology decreases and the bandwidth needs of metro networks increase. From the management, craft training, and equipment inventory perspectives, it is desirable to have as much commonality as possible between core and metro networks when they exist within the same carrier. LECs typically have both metro networks and core networks to provide interconnection within their region. IECs also typically have both metro and core networks since they often deploy metro networks in order to more efficiently reach their business/corporate subscribers.

As shown in Figure, both metro and core transport networks can consist of ring and mesh topologies. Rings have become increasingly popular since they provide inherent route diversity that can be exploited for protection switching. (See City 1 and upper portion of the core network.) Rings have also become increasingly popular in access networks (e.g., City 3). Traffic routing on rings is also more straightforward than in arbitrary mesh networks.

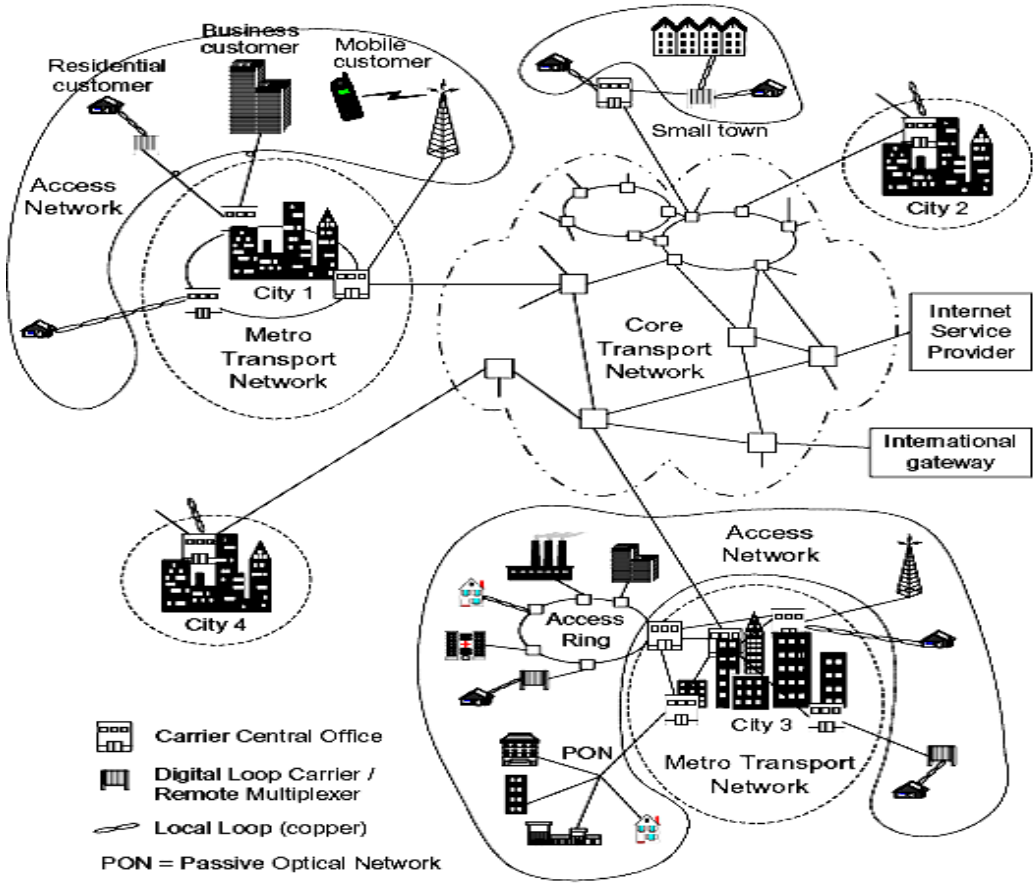


Figure 94: **Illustration of a telecommunications network**

Ring topologies are not always convenient, however, due to such constraints as geography or having to use pre-existing right of ways. Arbitrary mesh networks are constructed in order to use convenient cable routings or, in some cases, allow more bandwidth-efficient protection schemes. Transport networks often consist of a mix of ring and mesh sub-networks, including interconnected rings. The switches provide the automatic routing of voice (or data) traffic, while the transmission equipment handled the multiplexing and facility connections to carry the traffic between the switches. For example, a voice switch is the equipment to which a subscriber's telephone is connected that does the digit collection when the subscriber dials, and routes the call according to the number that was dialed. Typical transmission equipment includes SONET/SDH terminals. The distinction between transmission and switching has continued to blur over the past 20 years. Transmission networks have increasingly deployed digital cross connect systems (DCSs) that switch subscribers' traffic between the various DCS interfaces according to a provisioned route. DCS-type cross-connect capability has increasingly been integrated into add-drop multiplexers (ADMs).

16.4 TRANSPORT NETWORK AND THE ROAD ANALOGY

The transport network is analogous to any road network of a country. The national highway of a country has a greater capacity for vehicle traffic than the state highway and the city roads. The state highway has less vehicle traffic-carrying capacity than the city road network. Analogous to this, the access part of a transport network has less capacity than the metro network and the metro part has less capacity than the core part of the transport network..

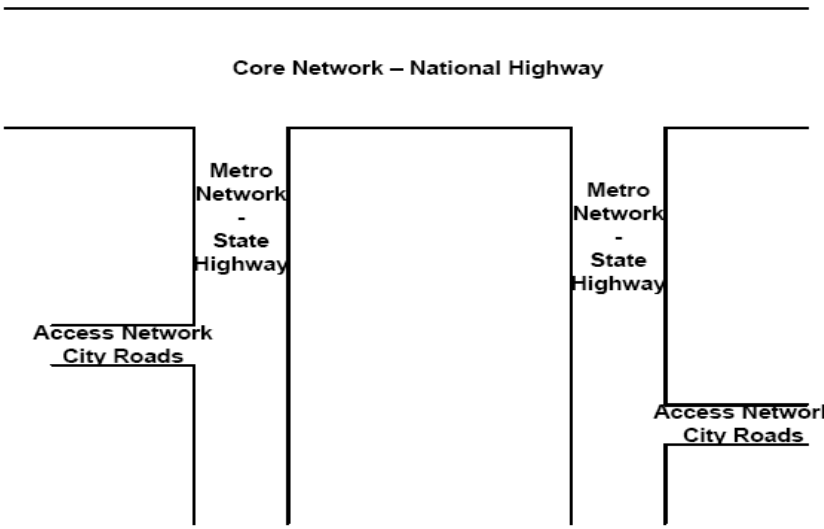


Figure 95: **Transport Network and Road Analogy**

The evolution of transport technology with the increase in bandwidth demand .

The analog voice was digitized and the Plesiochronous Digital (PDH) techniques were discovered for the transportation of information. Though, these techniques were popular in the old days, the increasing demand for bandwidth proved that these techniques have many drawbacks. The highest data rate available in PDH is 140 Mbps and the hardware required for multiplexing and demultiplexing of the signal is much more than that of in SDH/SONET due to the Plesiochronous signals. All these drawbacks of the PDH techniques carved the way for today's SDH/SONET techniques for information transportation over the telecom networks. Both SDH and SONET techniques are widely used due to their efficiency and reliability. Today's metro area networks (MANs) are built on legacy SONET/SDH ring infrastructure and both the SDH & SONET are used to transmit data over voice-optimized SDH/SONET network resulting in the wastage of bandwidth. The SDH/SONET networks lack the dynamic functionality and rapid scalability needed to cope-up with the increasing volumes and unpredictable bandwidth demands. Also, due to the rigid multiplexing hierarchies in the SDH/SONET standards, the customer cannot avail the flexible data rates and has to pay more. The next available bandwidth in a SDH network after 10 Gbps is 40 Gbps. e.g. - A customer, who requires, says 20 Mbps, actually has to subscribe to a 45 Mbps service because of the rigidity in the multiplexing hierarchy, resulting in the wastage of bandwidth and ending up paying bill for 45 Mbps link.

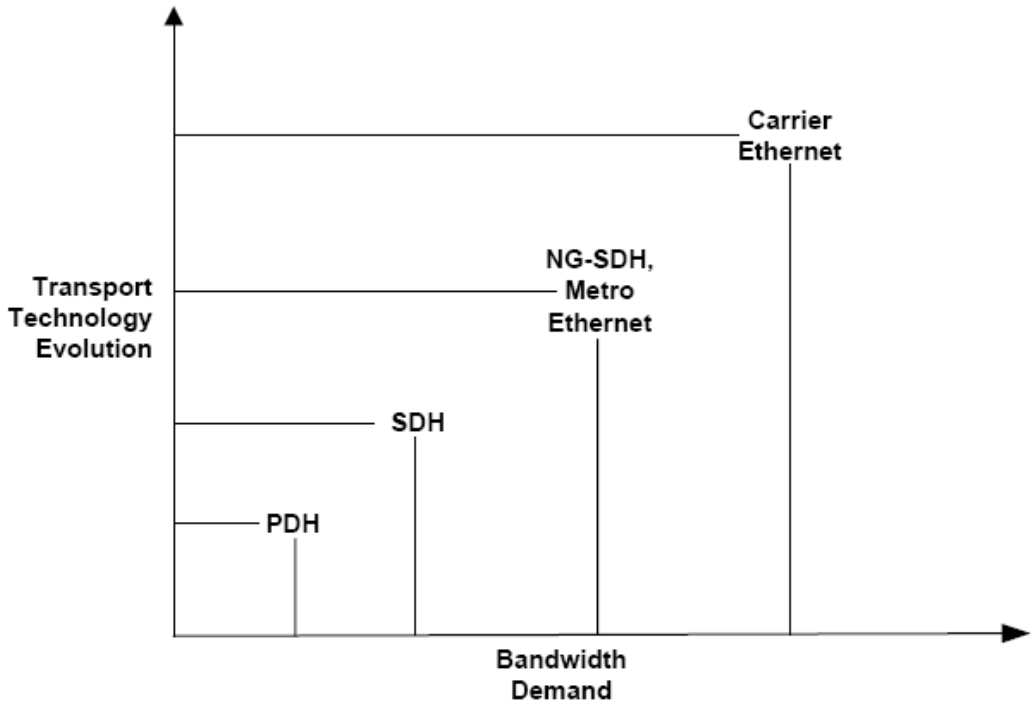


Figure 96: **Transport Technologies Evolution**

Also, customer may demand extra bandwidth for a limited period of time and may again switch back to a low bandwidth service. The service activation and service provisioning in both the cases should be quick enough to satisfy the customer's demands. The ports of SDH/SONET network elements are not programmable and the bandwidth offered by

these ports cannot be changed dynamically. If a subscriber changes his bandwidth demand, the port from which he is getting the service needs to be changed physically. This is very time-consuming. e.g. – An enterprise customer is having a STM-4 connection initially and he needs to upgrade it to STM-16 for one month only. The service provisioning and service activation for this requirement should be quick enough to fulfill the requirement of the customer in minimum time so that his business is not affected and the customer enjoys the flexibility in the service. Also, the time required to revert back to the original low bandwidth requirement should be very less. Time required for designing, deploying and maintaining a separate voice and data network is very high. To isolate and diagnose the faults through a complex hierarchical network is a cumbersome task and the operational expenses to maintain these separate voice and data networks are very high as it needs a larger workforce.

Considering the limitations of SDH/SONET, what is needed are ways to manage data-service bandwidth dynamically in small increments, to provide a range of service guarantees, and to engineer traffic flows more efficiently. So to improve SDH/SONET into a new generation, while keeping its essential virtues, the main technological focus is on devising new client-service encapsulations and scrapping the traditional multiplexing/mapping scheme, replacing it with a more flexible alternative within the basic SDH/SONET framing.

16.5 TRANSPORT TECHNOLOGIES FOR NEXT GENERATION TELECOM NETWORKS

A solution to handle the increasing data traffic effectively can be building a brand-new data-based infrastructure. Carriers, however, have done significant investments in their existing SONET/SDH core infrastructures. This investment has run to hundreds of billions of dollars over a significant period of time. Hence, throwing the existing infrastructure away and building a new one is not feasible.

16.5.1 Multi-Service Provisioning Platform (MSPP)

One feasible approach to handle the continuously increasing data traffic can be to adapt the existing SDH/SONET based infrastructure for data. By replacing SONET/SDH add/drop multiplexers (ADMs) with multi-service provisioning platforms (MSPP) that support Ethernet and other packet-based protocols, as well as TDM and multiple optical wavelengths, carriers can achieve significant returns on their scarce investment dollars. This approach today is known as the Next-Generation SDH/SONET. It came into existence around 2002. MSPP has the following advantages.

- Using MSPP, carriers can take the advantage of fiber optic capabilities to provide higher levels of service density.

- Legacy TDM and optical network support for all restoration techniques, topologies, and transmission criteria.
- No need to implement overlay networks.
- MSPP provides rapid end-to-end service provisioning and efficient OAM functions reducing the management overhead and expenditure by reducing the service deployment time.
- Cost-effective as a single box can take care of the TDM, packet as well as wavelength services.

16.5.2 Metro Ethernet

Another approach is to use Ethernet in the metro networks, which is called Metro Ethernet. Ethernet is a very popular technology and if combined with the fiber optic technology can be used to provide carrier-class services as well as traditional Ethernet services (10 Mbps, 100 Mbps, and/or 1 Gbps). With this approach, we can leverage the advantage of familiarity and ubiquity of Ethernet networking with the speed of optical transport. Using Ethernet can give the cost benefit to both, Service Providers and subscribers in the following two ways:

- The Ethernet interfaces itself are very less expensive due to its broad usage in almost all networking products.
- Many Ethernet services allow subscribers to add bandwidth in granular increments. Bandwidths are scalable from 1 Mbps to 100 Gbps and beyond, and subscribers can add bandwidth as needed and pay only for what the need.

Today, there are various Ethernet applications and services and several service technologies are used for metro Ethernet service delivery.

16.5.3 Ethernet Over Sonet/Sdh (EOS)

Ethernet over SONET/SDH is typically used for private line applications. It is a point-to-point service with a native Ethernet interface. EoS was developed as a packet data transport solution which would allow the use of the existing deployed SONET/SDH infrastructure.

Over the past several years, a series of new protocols such as Generic Framing Procedures (GFP), Virtual Concatenation (VACT), Link Capacity Adjustment Schemes (LCAS) have emerged that facilitate far more flexible, efficient provisioning of P2P Ethernet circuits over SDH. Some of the benefits of EoS are simple provisioning, high security and high availability due to SDH protection mechanism, high granularity and relatively low cost.

16.5.4 Ethernet Over Dwdm (EoDWDM)

EoW is a point-to-point Ethernet Private Line (EPL) service. It is used when carriers need to offer ultra-high bandwidth services (GigE level and up) to connect customers' data centers and allow large file transfers between corporate sites, such as storage network applications. It is also used for applications, such as video transport, and to provide high fiber relief. EoW is deployed using either DWDM or CWDM. EoW offers high potential resiliency by providing protection at less than 50 msec. Service providers can offer Ethernet over WDM service at 1 Gbps and 10 Gbps.

16.5.5 Ethernet Over Fiber (EoF)

EoF is primarily deployed in a point-to-point or mesh network technology, and used to deliver packet services over fibers. It is a connectionless technology. It is usually used for LAN or Internet access connectivity.

The main benefit of EoF is low cost. Even though EoF is very cost effective, it lacks the reliability, manageability, and scalability of a traditional SDH solution.

16.5.6 Ethernet Over Resilient Packet Rings (RPR)

RPR is a technology similar to SONET/SDH and optimizes the sharing of fiber optic rings for packet data traffic. RPR uses a single ring technology in order to overcome multi-drop limitations of the point-to-point nature of Ethernet. However, RPR supports only ring configuration and is a single ring protocol. It does not support mesh and star topology. Also, RPR is not competent with the low cost of the equivalent Ethernet products.

16.5.7 Provider Backbone Transport (PBT)/PBB-TE

PBT is also known as Provider Backbone Bridge – Traffic Engineering (PBB-TE). It is a point-to-point Ethernet tunneling technology. PBT intends to offer SONET/SDH-like performance. PBT is more suitable for point-to-point business applications and MP2MP is not supported.

16.5.8 Ethernet Over Mpls (EoMPLS)

Multi-protocol label switching is a protocol that provides an efficient forwarding and switching of traffic flows through the network. MPLS technology enables service providers to build a cost-effective carrier-class Ethernet network over a new and/or existing SONET/SDH network, supporting any Ethernet-based applications and services. EoMPLS supports P2P and MP2MP service, P2MP hub and spoke service and rooted multicast. EoMPLS reduces CAPEX and OPEX and helps operators to build real converged networks. Metro Ethernet technologies, however pose many scalability and reliability challenges. The following are some of the issues that arise with Metro Ethernet networks:

- Restrictions on the number of customers
- Lack of Service monitoring
- Scaling the L2 backbone is almost impossible.
- Service provisioning
- Inter-working with legacy deployments

16.5.9 Carrier Ethernet

One more approach is use of Carrier Ethernet. The Metro Ethernet forum has defined Carrier Ethernet as a ubiquitous, standardized, carrier-class Service and Network defined by five attributes namely Standardized Services, Scalability, Reliability, Quality of Service and Service Management that distinguish Carrier Ethernet from familiar LAN based Ethernet. The carrier-class services can be provided by using Carrier Ethernet in the network. Standardized Services attribute of the Carrier Ethernet essentially enables a Service Provider to deliver a host of both Packet and traditional TDM multi-point services in an efficient and deterministic manner over standardized equipment platforms. These services make a foundation for number of customer applications that are emerging across voice, data and video. Carrier Ethernet solutions are more scalable in terms of users/endpoints, geographical reach, applications (business, information, and entertainment applications) and bandwidth Carrier Ethernet services are reliable as it addresses the reliability aspects of the service resiliency, protection and restoration. Hence, Carrier Ethernet services are expected to support mission-critical applications on a wide scale due the ability to detect quickly and remotely any failures that may arise in the physical infrastructure or in the Ethernet services layer underlying these applications. Carrier Ethernet is able to provide Quality of Service encompassing the Performance Service Level Agreement (SLA), SLA parameters and provisioning SLAs. Managing a large number of customers stretched over a wider geographical area requires Service Providers to have a sophisticated capability for installing, troubleshooting, and upgrading Ethernet services cost effectively and quickly makes it infeasible to deliver Ethernet on a wider scale. Carrier Ethernet addresses unified management, carrier-class OAM and rapid provisioning for the better service management.

Benefits of Carrier Ethernet-

- Use of Ethernet at Metro and carrier networks brings in the simplicity in the networks.
- These networks are more flexible and reliable than the legacy networks.
- The OAM of the network is simplified.
- The simplified Ethernet technology brings lower cost and products.

16.5.10 OTN Technology

The Optical Transport Network (OTN) standards, defined by the ITU-T G.709 standards, were developed to add SONET-like performance monitoring, fault detection, communication channels, and multiplexing hierarchy to WDM wavelengths. The primary benefits of OTN include:

- Enhanced OAM for wavelengths
- Universal container supporting any service type
- Standard multiplexing hierarchy
- End-to-end optical transport transparency of customer traffic
- Multi-level path OAM

16.5.11 CPAN

CPAN (Converged Packet Access Network) is based on MPLS-TP Technology. It is used for MPLS-TP aggregation network and access network. CPAN is a converged multi-service connection-oriented transport over packet technology of telecommunication system. It has combined feature of Packet network and SDH/SONET network.

Advantages of CPAN Technology:-

- Efficient bandwidth utilization,sharing bandwidth between services
- Includes the benefits of RPR.
- SDH packet switching based on statistical multiplexing.
- Path protection & recovery within 50 ms for any topology-Ring,Linear
- Support for TDM interfaces(E1,STM-1) & Multiservice traffic
- Both UNI & NNI interface upto max 100G capacity
- Access to last mile connectivity bandwidth upto 100G capacity.
    - bandwidth scalability -from 6G,40G to 100G
- OAM & Performance Monitoring-Proactive & Reactive
- Resiliency-1:1,1+1;Linear & Ring.
- GUI EMS provisioning.

16.6 ROADMS

Use of ROADM by the carriers is becoming popular. ROADM is nothing but Reconfigurable Add/Drop Multiplexers. It eliminates the pain associated with the legacy DWDM networks. DWDM falls short of scalability whenever there is a requirement to upgrade the DWDM network. ROADM provide an automated mechanism to flexibly add capacity, in terms of wavelengths, as it is needed, without interrupting the service.

ROADMs give network administrators the ability to select via software which of 32 DWDM channels to add, drop or pass-through at each site and dynamically provision an end-to-end, inter-office connection that can travel thousands of miles, across a DWDM

SDH/SONET ring in their metro and access networks. This lets them seamlessly add services as end-user demand necessitates.

ROADM maps wavelengths from metro access through metro core using emerging generic multi-protocol label switching (G-MPLS) control plane standards. Eventually, it could take over all grooming of traffic above STM-1 (155 Mbps) speeds and push the SDH/SONET ADM's traditional job of grooming sub-wavelength E-1 and E-3 traffic out of the core toward the customer.

The concept of ROADM is still undergoing a lot of dramatic changes and the vendors are coming out with proprietary stuff.

16.7 ALL-OPTICAL CORE NETWORKS

Over the last few years, optical fiber has become the transmission medium of choice because it provides large bandwidth {approximately 24 Tera Hertz (THz)}, low attenuation, and low Bit Error Rate (BER) (less than 10-11). In today's networks, electronic devices such as switches and routers are interconnected by optical fiber links.

A major limitation of these types of networks, often referred to as electro-optic networks, is “electronic bottleneck”. This electronic bottleneck is caused by the fact that information transfer involves time-consuming processes of optical-to-electronic conversion, electrical signal processing and electronic-to- optical conversion of data signals at intermediate optical nodes. Additionally, all of the information carried on optical fibers must be processed at electronic data rates that are compatible with electronic circuitry (in the order of few Gigabits per Second (Gb/s)), thereby limiting Network throughput. Over the last decade, processors and other related peripherals have advanced in speed by two orders of magnitude, however electronic interconnecting devices such as switches and routers by only one order of magnitude. Therefore, the amount of information that can be carried over an optical fiber link is limited by the information processing speed of the interconnecting electronic devices used at each end of the link and not by the fiber itself. Recently, a new concept, called all-optical networking, has been developed to overcome these effects. Using this concept, information can be transmitted using optical signals and without optical -to-electronic conversion and vice versa. Networks constructed using this concept are called AONs.

All-optical networks (AONs) are a viable technology for future telecommunication and data networks, an all-optical network (AON) is a network that uses light wave communication exclusively within the network. More precisely, in an AON all network-to network interfaces are based on optical transmission, all user-to-network interfaces use optical transmission on the network side of the interface, and all switching and routing within AON network nodes is performed optically. The principal advantage of maintaining an optical network core in comparison to using electro-optic components at nodes or in transmission systems is higher bandwidth: optical bandwidths

are generally one thousand fold those of electronic bandwidths, and avoiding optical/electronic/optical conversions therefore promises roughly one thousand times greater data rates than possible with electro-optic networks. Transparency is an optical network feature that allows routing and switching of data within the network without interpretation or regeneration of the individual data streams. While transparency has many desirable features (e.g. terminal upgrades do not require network upgrades), it has important ramifications for security.

AON architecture can generally be divided into optical terminals (which are the user-network interface), network nodes (which switch, route, and sometimes perform mux/demux), and optically amplified fiber optic links. A separate control network (not always all-optical) is usually used for signaling purposes. The switching and routing may be done via mechanical switches, opto-electronic switches, passive optical routers, or splitter/combiners. Common topologies include star, ring, and mesh. Some of the architectures allow a hybrid mixture of topologies. A particularly important component is the optical amplifier. Amplifiers are used in both nodes and links of AONs. It is worth noting that although AONs are not generally commercial products today, each of the above components is commercially available from multiple manufacturers. All optical networks are very often considered to be the main candidate for constituting the backbone that will carry global data traffic whose volume has been growing at astounding rates that are not expected to slow down in the near future. According to the physical technology employed, one can identify three generations of networks.

Networks built before the emergence of optical fiber technology are the first generation networks (i.e. networks based on copper wire or radio).

The second generation networks employ fibers in traditional architectures. The choice of fiber is due to its large bandwidth, low error rate, reliability, availability, and maintainability. Although some performance improvements can be achieved by employing fibers, the performance for this generation is limited by the maximum speed of electronics (a few gigabits per second) employed in switches and end-nodes. This phenomenon is called an *electronics bottleneck*. In order to satisfy the increasing bandwidth requirements of emerging applications, totally new approaches are employed to exploit vast bandwidth (approximately 30THz in the low loss region of single mode fiber in the neighborhood of 1500nm) available in fibers.

Therefore, the third generation networks are designed as *all-optical* to avoid the electronics bottleneck. That is, information is conveyed in the optical domain (without facing any electro-optical conversions) through the network until it reaches its final destination. The emergence of single mode fibers, all-optical wide-band amplifiers, optical couplers, tunable lasers (transmitters)/filters (receivers), and all-optical cross-connects enable the realization of third generation networks. In order to make use of the vast bandwidth available without experiencing electronics bottleneck, concurrency among

multiple user transmissions can be introduced. In all-optical networks, concurrency can be supplied through time slots (OTDM-optical time division multiplexing), wave shape (CDM-code division multiplexing) or wavelength (WDM-wavelength division multiplexing).

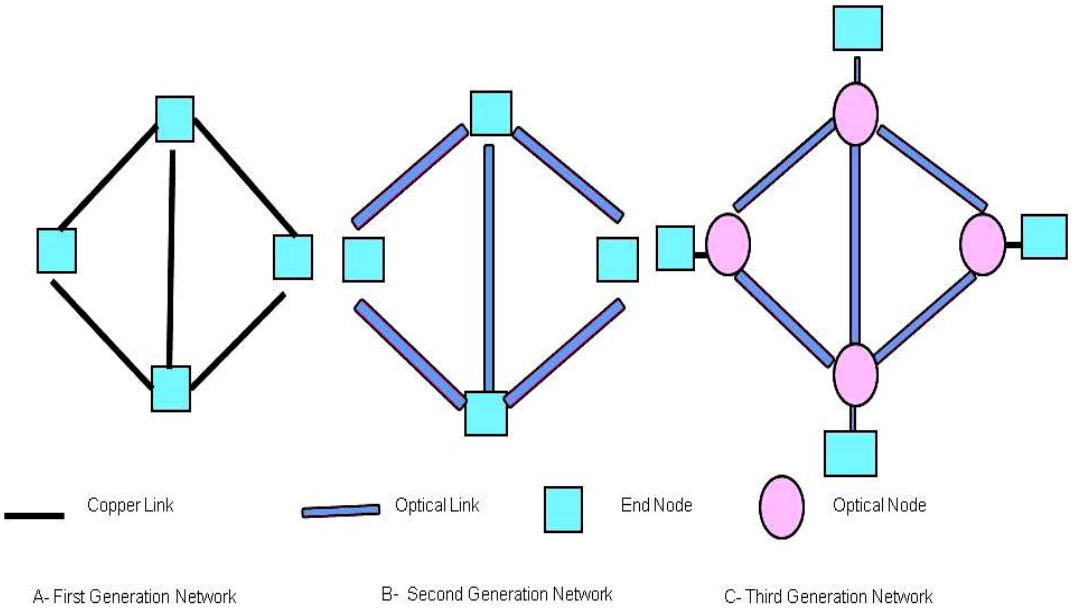


Figure 97: **Three Generation of Networks**

In AONs, as the name indicates, information is transmitted entirely in optical form. There are no optical/electronic conversions within the network. One major advantage of AONs with respect to their electro-optic counterparts is their much higher bandwidth. Elimination of electronic/optical conversion reduces delays, increases capacity, and improves flexibility of networks. In this regard, AONs are a natural solution to the ever-increasing demand for higher speeds and larger capacities. At present, optical transmission links supporting 100 Gb/s are commercially available.

16.8 AUTOMATICALLY SWITCHED OPTICAL NETWORK (ASON)

ASON (Automatically Switched Optical Network) is a concept for the evolution of transport networks which allows for dynamic policy-driven control of an optical or SDH network based on signaling between a user and components of the network. Its aim is to automate the resource and connection management within the network.

In an optical network without ASON, whenever a user requires more bandwidth, there is a request for a new connection. The service provider must then manually plan and configure the route in the network. This is not only time consuming, but also wastes bandwidth if the user sparingly uses the connection. Bandwidth is increasingly becoming a precious resource and expectations from future optical networks are that they should be able to efficiently handle resources as quickly as possible. ASON fulfills some of the requirements of optical networks such as:

- Fast and automatic end-to-end provisioning
- Fast and efficient re-routing
- Support of different clients, but optimized for IP
- Dynamic set up of connections
- Support of Optical Virtual Private Networks (OVPNs)
- Support of different levels of quality of service .

16.9 CONCLUSION

Optical Transport Networking is a telecommunication industry-standard protocol which provides a way of multiplexing different services onto optical light paths. It was originally designed to promote network evolution beyond SONET/SDH.. As network service providers tackle the ever-increasing issue of rapid user growth and increasing digital traffic, with such things as mobile apps, social media, cloud computing, VoIP and video calling, technological solutions such as OTN are being adapted.

17 SDH TECHNOLOGY

17.1 LEARNING OBJECTIVES

•Limitation of PDH signals.

•Concept of SDH.

•Multiplexing Structure of STM.

17.2 INTRODUCTION

With the introduction of PCM technology in the 1960s, communications networks were gradually converted to digital technology over the next few years. To cope with the demand for ever higher bit rates, a multiplex hierarchy called the Plesiochronous digital hierarchy (PDH) evolved. The bit rates start with the basic multiplex rate of 2 Mbit/s with further stages of 8, 34 and 140 Mbit/s. In North America and Japan, the primary rate is 1.5 Mbit/s. Hierarchy stages of 6 and 44 Mbit/s developed from this. Because of these very different developments, gateways between one network and another were very difficult and expensive to realize. PCM allows multiple use of a single line by means of digital time-domain multiplexing. The analog telephone signal is sampled at a bandwidth of 3.1 kHz, quantized and encoded and then transmitted at a bit rate of 64kbit/s. A transmission rate of 2048 kbit/s results, when 30 such coded channels are collected together into a frame along with the necessary signaling information. This so-called primary rate is used throughout the world. Only the USA, Canada and Japan use a primary rate of 1544 kbit/s, formed by combining 24 channels instead of 30. The growing demand for more bandwidth meant that more stages of multiplexing were needed throughout the world. A practically synchronous (or, to give it its proper name: plesiochronous) digital hierarchy is the result. Slight differences in timing signals mean that justification or stuffing is necessary when forming the multiplexed signals. Inserting or dropping an individual 64 kbit/s channel to or from a higher digital hierarchy requires a considerable amount of complex multiplexer equipment.

Traditionally, digital transmission systems and hierarchies have been based on multiplexing signals which are plesiochronous (running at almost the same speed). Also, various parts of the world use different hierarchies which lead to problems of international interworking; for example, between those countries using 1.544 Mbit/s systems (U.S.A. and Japan) and those using the 2.048 Mbit/s system. To recover a 64 kbit/s channel from a 140 Mbit/s PDH signal, it's necessary to demultiplex the signal all the way down to the 2 Mbit/s level before the location of the 64 kbit/s channel can be identified. PDH requires "steps" (140-34, 34-8, 8-2 demultiplex; 2-8, 8-34, 34-140 multiplex) to drop out or add an individual speech or data channel

17.3 PLESIOCHRONOUS DIGITAL MULTIPLEXING

PDH technology (Plesiochronous Digital Hierarchy) is based on pulse code modulation (PCM). In pulse code modulation a multiple-shift usage of a transmission link is enabled by TDM (time division multiplexing). PDH technology enables with its hierarchical structures the implementation of networks with transmission capacities of up to 140 Mbit/s. In applications with cross connecting on bit-level or with a demand of special interfaces, PDH system technology is in use even today.

Traditionally, transmission systems have been asynchronous, with each terminal in the network running on its own clock. In digital systems, clocking (timing) is one of the most important considerations. Timing means using a series of repetitive pulses to keep the bit rate of the data stream constant and to indicate where the ones and zeros are located in a data stream. Because these clocks are free running and not synchronized, large variations occur in the clock rate and thus the signal bit rate.

Asynchronous multiplexing uses multiple stages; lower-rate signals are multiplexed, and extra bits are added (bit-stuffing) to account for the variations of each individual stream and combined with other bits (framing bits) to form higher-level bit rates. Then bit-stuffing is used again to produce even higher bit rates. At the higher asynchronous rate, it is impossible to access these signals without multiplexing.

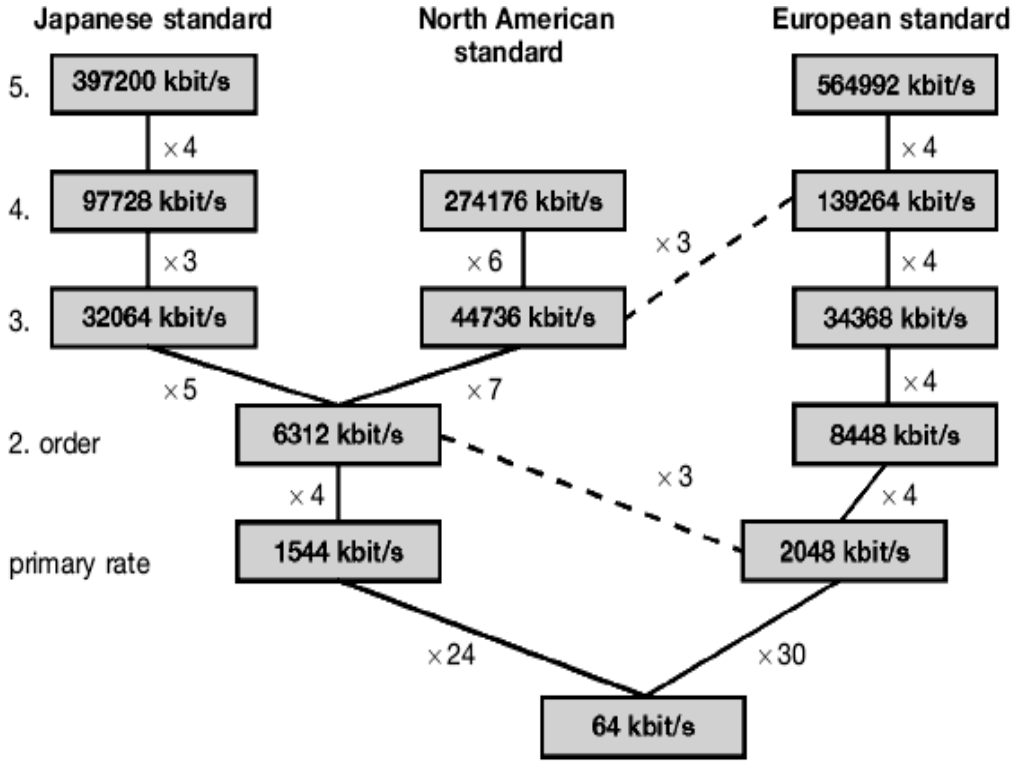


Figure 98: **Plesiochronous Digital Hierarchies (PDH)**

The Plesiochronous Digital Hierarchy (PDH) signals have the essential characteristics of time scales or signals such that their corresponding significant instants occur at nominally the same rate. The prefix plesio, which is of Greek origin, means "almost equal but not exactly," meaning that the higher levels in the CCITT (ITU today) hierarchy are not an exact multiple of the lower level. Any variation in rate is constrained within specified limits. The PDH systems belong to the first generation of digital terrestrial telecommunication systems in commercial use.

Before SDH transmission networks were based on the PDH hierarchy. 2 Mbit/s service signals are multiplexed to 140 Mbit/s for transmission over optical fiber or radio. Multiplexing of 2 Mbit/s to 140 Mbit/s requires two intermediate multiplexing stages of 8 Mbit/s and 34 Mbit/s. Multiplexing of 2 Mbit/s to 140 Mbit/s requires multiplex equipment known as 2nd, 3rd and 4th order multiplexer.

17.4 S.D.H. EVOLUTION

SDH evolution is possible because of the following factors:

(i) **Fibre Optic Bandwidth:** The bandwidth in Optical Fibre can be increased and there is no limit for it. This gives a great advantage for using SDH.

(ii) **Technical Sophistication:** Although, SDH circuitary is highly complicated, it is possible to have such circuitary because of VLSI technique which is also very cost effective.

(iii) **Intelligence:** The availability of cheaper memory opens new possibilities.

(iv) **Customer Service Needs:** The requirement of the customer with respect to different bandwidth requirements could be easily met without much additional equipment.

The different services it supports are:

1. Low/High speed data.
2. Voice
3. Interconnection of LAN
4. Computer links
5. Broadband ISDN transport (ATM transport)

17.5 ADVANTAGES OF SDH

SDH brings the following advantages to network providers:

17.5.1 High Transmission Rates

Transmission rates of up to 40 Gbit/s can be achieved in modern SDH systems. SDH is therefore the most suitable technology for backbones, which can be considered as being the super highways in today's telecommunications networks.

17.5.2 Simplified Add & Drop Function

Compared with the older PDH system, it is much easier to extract and insert low-bit rate channels from or into the high-speed bit streams in SDH. It is no longer necessary to demultiplex and then remultiplex the plesiochronous structure.

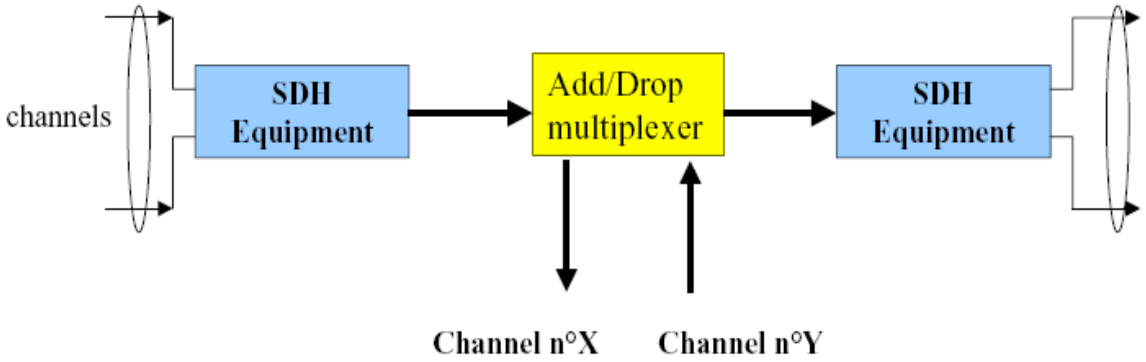


Figure 99: **Simplified add & drop function**

17.5.3 High Availability And Capacity Matching

With SDH, network providers can react quickly and easily to the requirements of their customers. For example, leased lines can be switched in a matter of minutes. The network provider can use standardized network elements that can be controlled and monitored from a central location by means of a telecommunications network management (TMN) system.

17.5.4 Reliability

Modern SDH networks include various automatic back-up and repair mechanisms to cope with system faults. Failure of a link or a network element does not lead to failure of the entire network which could be a financial disaster for the network provider. These back-up circuits are also monitored by a management system.

17.5.5 Future-Proof Platform For New Services

Right now, SDH is the ideal platform for services ranging from POTS, ISDN and mobile radio through to data communications (LAN, WAN, etc.), and it is able to handle the very latest services, such as video on demand and digital video broadcasting via ATM that are gradually becoming established.

17.5.6 Interconnection

SDH makes it much easier to set up gateways between different network providers and to SONET systems. The SDH interfaces are globally standardized, making it possible

to combine network elements from different manufacturers into a network. The result is a reduction in equipment costs as compared with PDH.

17.5.7 Support PDH Payloads

SDH supports the transmission of existing PDH payloads, other than 8Mbit/s. Most importantly, because each type of payload is transmitted in containers synchronous with the STM-1 frame, selected payloads may be inserted or extracted from the STM-1 or STM-N aggregate without the need to fully hierarchically de-multiplex as with PDH systems.

17.6 SDH RATES

SDH is a transport hierarchy based on multiples of 155.52 Mbit/s. The basic unit of SDH is STM-1. Different SDH rates are given below:

STM-1 = 155.52 Mbit/s

STM-4 = 622.08 Mbit/s

STM-16 = 2588.32 Mbit/s

STM-64 = 9953.28 Mbit/s

Each rate is an exact multiple of the lower rate therefore the hierarchy is synchronous.

17.7 THE STM-1 FRAME FORMAT

The S.D.H. standards exploit one common characteristic of all PDH networks namely 125 micro seconds duration, i.e. sampling rate of audio signals (time for 1 byte in 64 k bit per second). This is the time for one frame of SDH. The frame structure of the SDH is represented using matrix of rows in byte units as shown. As the speed increases, the number of bits increases and the single line is insufficient to show the information on Frame structure. Therefore, this representation method is adopted. How the bits are transmitted on the line is indicated on the top of the figure.

The Frame structure contains 9 rows and number of columns depending upon synchronous transfer mode level (STM). In STM-1, there are 9 rows and 270 columns. The reason for 9 rows arranged in every 125 micro seconds is as follows:

For 1.544 Mbit PDH signal (North America and Japan Standard), there are 25 bytes in 125 micro second and for 2.048 Mbit per second signal, there are 32 bytes in 125 micro second. Taking some additional bytes for supervisory purposes, 27 bytes can be allotted for holding 1.544 Mbit per second signal, i.e. 9 rows x 3 columns. Similarly, for 2.048 Mbit per second signal, 36 bytes are allotted in 125 micro seconds, i.e. 9 rows x 4 columns. Therefore, it could be said 9 rows are matched to both hierarchies.

The standardized SDH transmission frames, called Synchronous Transport Modules of Nth hierarchical level (STM-N). The STM-1 frame is the basic transmission

format for SDH. The frame lasts for 125 microseconds; therefore, there are 8000 frames per second.

A frame with a bit rate of 155.52 Mbit/s is defined in ITU-T Recommendation G.707. This frame is called the synchronous transport module (STM). Since the frame is the first level of the synchronous digital hierarchy, it is known as STM-1. Figure 4 shows the format of this frame. It is made up from a byte matrix of 9 rows and 270 columns. Transmission is row by row, starting with the byte in the upper left corner and ending with the byte in the lower right corner. The frame repetition rate is 125 ms., each byte in the payload represents a 64 kbit/s channel. The STM-1 frame is capable of transporting any PDH tributary signal.

The first 9 bytes in each of the 9 rows are called the overhead. G.707 makes a distinction between the regenerator section overhead (RSOH) and the multiplex section overhead (MSOH). The reason for this is to be able to couple the functions of certain overhead bytes to the network architecture. The table below describes the individual functions of the bytes.

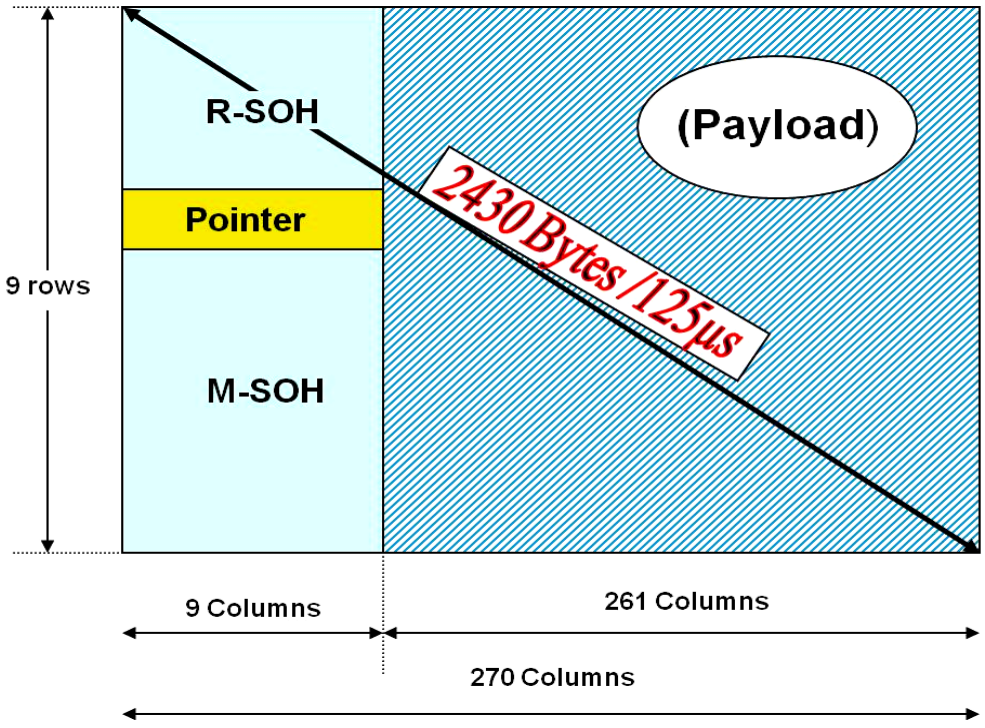


Figure 100: **Schematic diagram of STM-1 frame**

Calculation of Bit Rate of STM-1

- NO OF ROWS IN FRAME: 9
- NO OF COLUMNS: 270
- NO OF BYTES IN FRAME: 270*9
- NO OF BITS IN A FRAME: 270*9*8
- FRAME DURATION: 125us

- NO OF BITS TRANSMITTED IN ONE SECOND: 270*9*8*1/125 µs

=155.520Mb/S

17.8 SECTION OVERHEAD (SOH) AREA

The first 9 bytes in each of the 9 rows are called the overhead. SOH means the additional bytes in the STM-N frame structure needed for normal and flexible transmission of information payload and these bytes are mainly used for the running, management and maintenance of the network. In the 1~ 9 × N columns of the SDH frame, 1~3 rows and 5~9 rows are allocated to the SOH. SOH can be further categorized as RSOH (Regenerator Section Overhead) and MSOH (Multiplex Section Overhead). 1~3 rows are allocated to RSOH and 5~9 rows to MSOH. RSOH can be accessed either at the regenerator to at the terminal equipment. However, MSOH passes a regenerator transparently and is terminated at the terminal equipment. Fig. 3 shows distinction between the regenerator section overhead (RSOH) and the multiplex section overhead (MSOH).

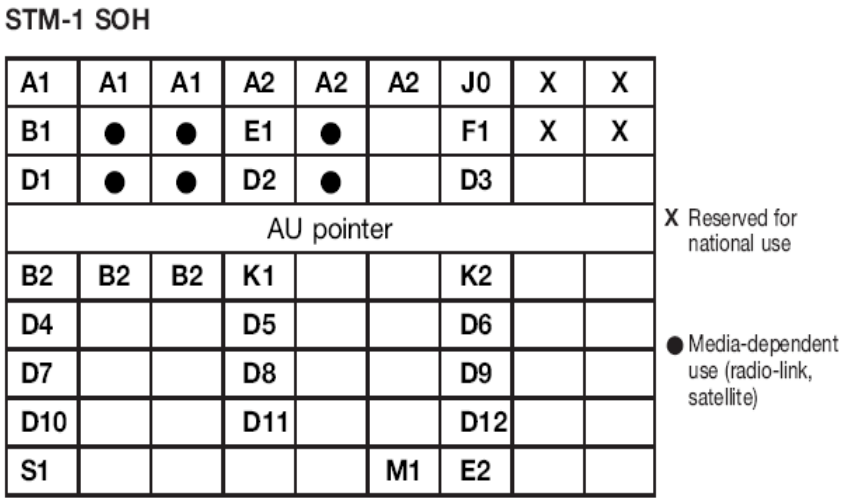


Figure 101: **Section Overhead**

The table below describes the individual functions of the bytes.

Overhead byte	Function
A1, A2	Frame alignment
B1, B2	Quality monitoring, parity bytes
D1 . . . D3	Q_{ECC} network management
D4 . . . D12	Q_{ECC} network management
E1, E2	Voice connection
F1	Maintenance
J0 (C1)	Trace identifier
K1, K2	Automatic protection switching (APS) control
S1	Clock quality indicator
M1	Transmission error acknowledgment

17.9 PAYLOAD AREA

Information payload area is the place where information about various services is stored in the SDH frame structure. Horizontal columns 10 × N~270 × N, and vertical rows 1~9 belong to the information payload area. In it, there are still some Path Overhead (POH) bytes transmitted as part of the payload in a network and these bytes are mainly used for the monitor, management and control of the path performance.

17.10 ADMINISTRATIVE UNIT POINTER (AU-PTR) AREA

AU PTR is a kind of indicator, mainly used to indicate the accurate position of the first byte of information payload in the STM-N frame, so that the information can be correctly decomposed at the receiving end. It is located at the fourth row of 1~9 × N columns in the STM-N frame structure. The adoption of the pointer mode is an innovation of SDH. It can perform multiplex synchronization and STM-N signal frame locating in the quasi-synchronization environment.

17.11 PATH OVERHEAD

Path Overhead (POH) bytes are mainly used for the monitor, management and control of the path performance. A distinction is made between two different POH types:

17.11.1 Vc-11/12 POH

The VC-11/12 POH is used for the low-order path. ATM signals and bit rates of 1.544 Mbit/s and 2.048 Mbit/s are transported within this path.

V5	Indication and error monitoring
J2	Path indication
N2	Tandem connection monitoring
K4	Automatic protection switching

17.11.2 Vc-3/4 POH

The VC-3/4 POH is the high-order path overhead. This path is for transporting 140 Mbit/s, 34 Mbit/s and ATM signals.

J1	Path indication
B3	Quality monitoring
C2	Container format
G1	Transmission error acknowledgment
F2	Maintenance
H4	Superframe indication
F3	Maintenance
K3	Automatic protection switching
N1	Tandem connection monitoring

17.12 NETWORK ELEMENTS OF SDH

Figure 4 is a schematic diagram of a SDH ring structure with various tributaries. The mixture of different applications is typical of the data transported by SDH. Synchronous networks must be able to transmit plesiochronous signals and at the same time be capable of handling future services such as ATM.

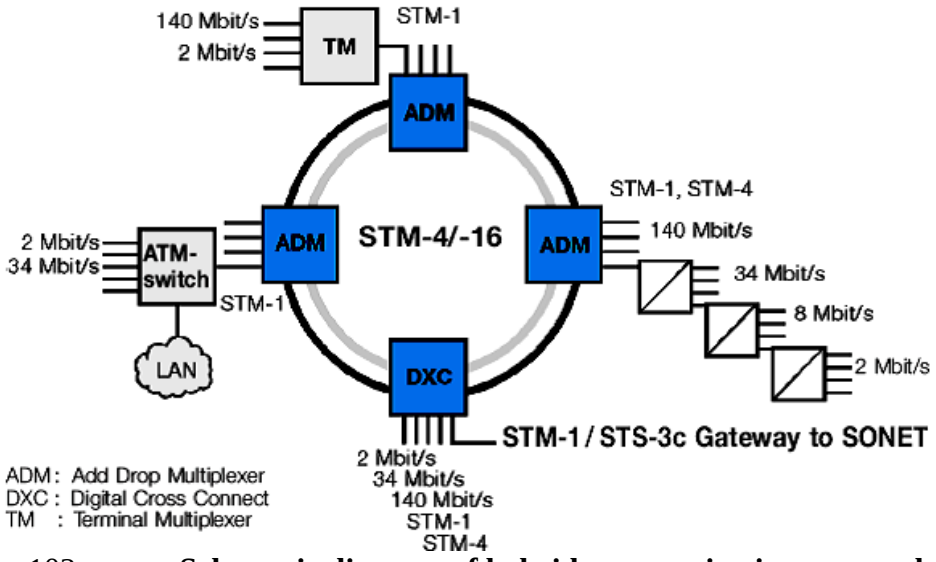


Figure 102: **Schematic diagram of hybrid communications networks**

Current SDH networks are basically made up from four different types of network element. The topology (i.e. ring or mesh structure) is governed by the requirements of the network provider.

17.12.1 Terminal Multiplexer (TM)

Terminal multiplexers are used to combine plesiochronous and synchronous input signals into higher bit rate STM–N signals as shown in Fig. 3 below. On the tributary side, all current plesiochronous bit rates can be accommodated. On the aggregate, or line side we have higher bit rate STM–N signals. Terminal multiplexers are used to combine plesiochronous and synchronous input signals into higher bit rate STM-N signals.

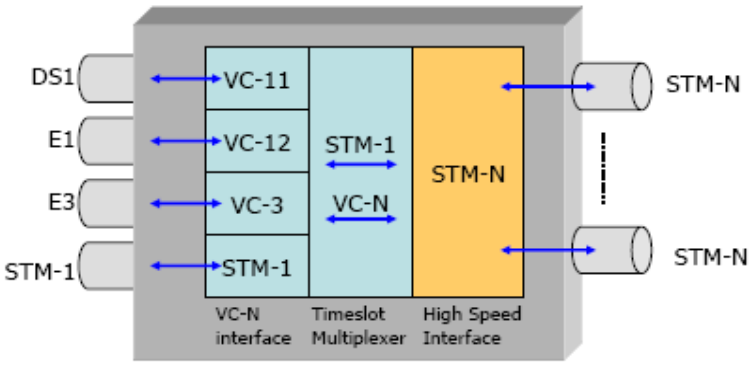


Figure 103: **Terminal Multiplexer**

17.12.2 Add/Drop Multiplexers(ADM)

Add/drop multiplexers (ADM**)** permits add and drop of lower order signals. Lower bit rate synchronous signals can be extracted from or inserted into high speed SDH bit streams by means of ADMs. This feature makes it possible to set up ring structures, which have the advantage that automatic back-up path switching is possible using elements in the ring in the event of a fault.

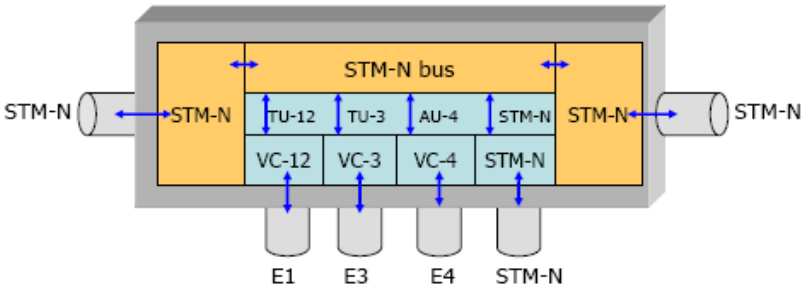


Figure 104: **ADM**

17.12.3 Regenerators

Regenerators as the name implies, have the job of regenerating the clock and amplitude relationships of the incoming data signals that have been attenuated and distorted by dispersion. They derive their clock signals from the incoming data stream. Messages are received by extracting various 64 kbit/s channels (e.g. service channels E1, F1) in the RSOH (regenerator section overhead). Messages can also be output using these channels.

Figure 105: **Regenerator**

17.12.4 Digital Cross-Connect (DXC)

This network element has the widest range of functions. It allows mapping of PDH tributary signals into virtual containers as well as switching of various containers up to and including VC-4. It permits switching of Transmission lines with different bit rates.

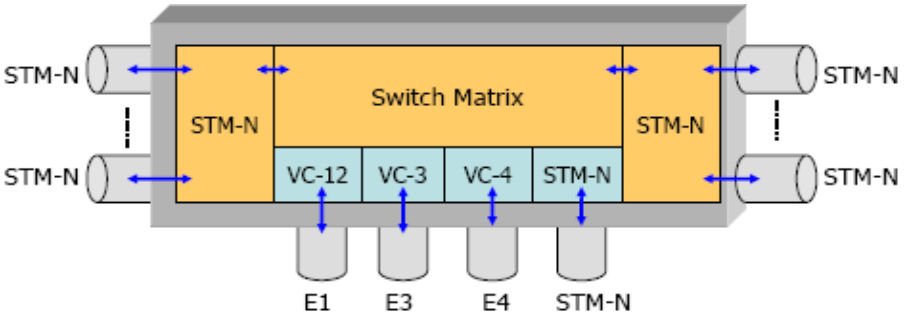


Figure 106: **DXC**

17.13 NETWORK ELEMENT MANAGER

Telecommunications management network (TMN) is considered as a further element in the synchronous network. All the SDH network elements mentioned so far are software-controlled. This means that they can be monitored and remotely controlled, one of the most important features of SDH.

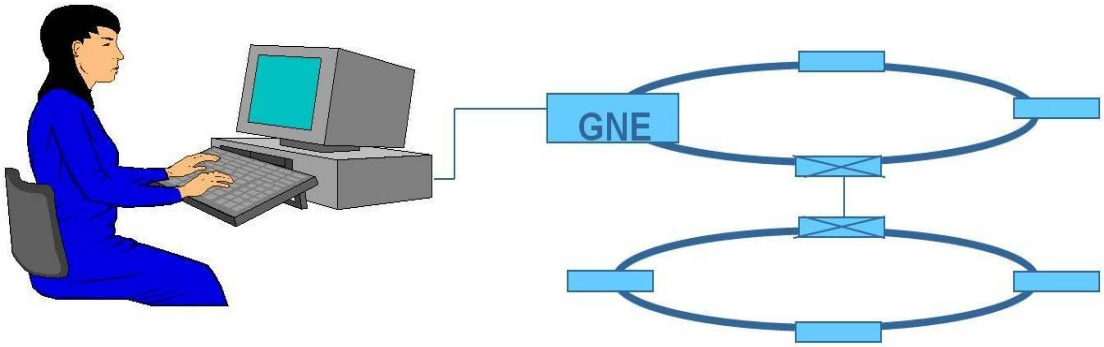


Figure 107: **Network Element Manager**

17.14 CONCLUSION

SDH (Synchronous Digital Hierarchy) is a standard technology for synchronous data transmission on optical media. It is the international equivalent of Synchronous Optical Network. Both technologies provide faster and less expensive network interconnection than traditional PDH (Plesiochronous Digital Hierarchy) equipment. Now Next Generation SDH is capable to support packet data also.

18 DENSE WAVELENGTH DIVISION MULTIPLEXING

18.1 LEARNING OBJECTIVES

•Concept of DWDM Technology.

•Network Architecture of DWDM

•Multiplexing Structure of DWDM.

18.2 INTRODUCTION

The emergence of DWDM is one of the most recent and important phenomena in the development of fiber optic transmission technology. Dense wavelength-division multiplexing (DWDM) revolutionized transmission technology by increasing the capacity signal of embedded fiber**.** One of the major issues in the networking industry today is tremendous demand for more and more bandwidth. Before the introduction of optical networks, the reduced availability of fibers became a big problem for the network providers. However, with the development of optical networks and the use of Dense Wavelength Division Multiplexing (DWDM) technology, a new and probably, a very crucial milestone is being reached in network evolution. The existing SONET/SDH network architecture is best suited for voice traffic rather than today's high-speed data traffic. To upgrade the system to handle this kind of traffic is very expensive and hence the need for the development of an intelligent all-optical network. Such a network will bring intelligence and scalability to the optical domain by combining the intelligence and functional capability of SONET/SDH, the tremendous bandwidth of DWDM and innovative networking software to spawn a variety of optical transport, switching and management related products.

18.3 DEVELOPMENT OF DWDM TECHNOLOGY

Early WDM began in the late 1980s using the two widely spaced wavelengths in the 1310 nm and 1550 nm (or 850 nm and 1310 nm) regions, sometimes called *wideband WDM*. The early 1990s saw a second generation of WDM, sometimes called *narrowband WDM,* in which two to eight channels were used. These channels were now spaced at an interval of about 400 GHz in the 1550-nm window. By the mid-1990s, dense WDM (DWDM) systems were emerging with 16 to 40 channels and spacing from 100 to 200 GHz. By the late 1990s DWDM systems had evolved to the point where they were capable of 64 to 160 parallel channels, densely packed at 50 or even 25 GHz intervals.

As shown in figure below the progression of the technology can be seen as an increase in the number of wavelengths accompanied by a decrease in the spacing of the

wavelengths. Along with increased density of wavelengths, systems also advanced in their flexibility of configuration, through add-drop functions, and management capabilities.

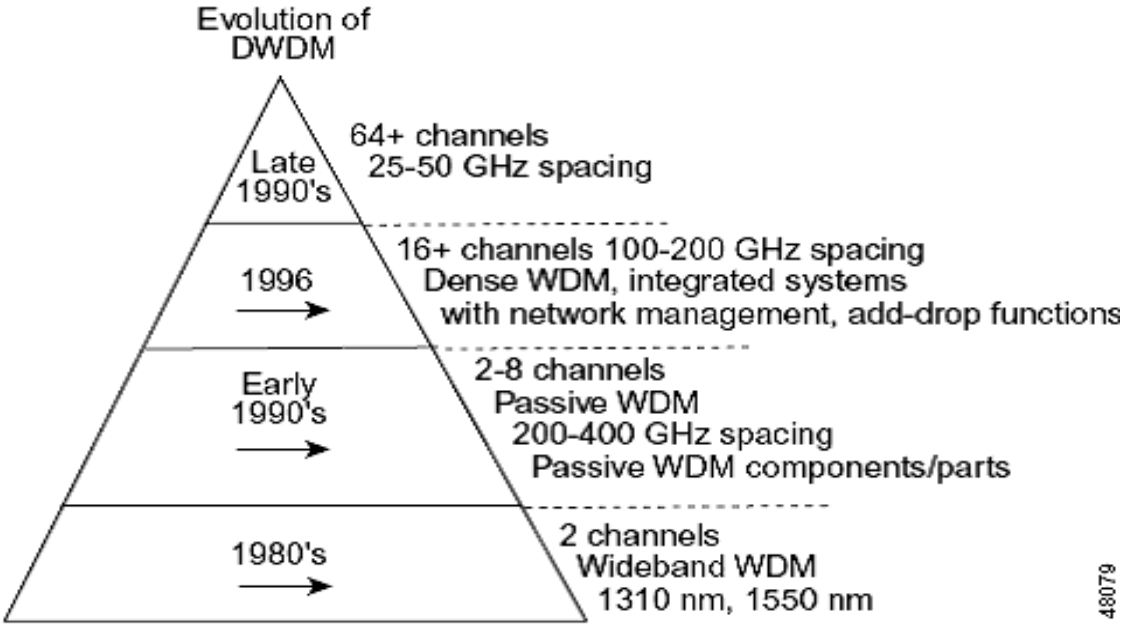


Figure 108: **Evolution of DWDM**

18.4 THE CHALLENGES OF TODAY'S TELECOMMUNICATIONS NETWORK

To understand the importance of DWDM and optical networking, these capabilities must be discussed in the context of the challenges faced by the telecommunications industry, and, in particular, service providers. The forecasts of the amount of bandwidth capacity needed for networks were calculated on the presumption that a given individual would only use network bandwidth six minutes of each hour. These formulas did not factor in the amount of traffic generated by Internet access (300 percent growth per year), faxes, multiple phone lines, modems, teleconferencing, and data and video transmission. In fact, today many people use the bandwidth equivalent of 180 minutes or more each hour.

Therefore, an enormous amount of bandwidth capacity is required to provide the services demanded by consumers. At the transmission speed of one Gbps, one thousand books can be transmitted per second. However today, if one million families decide they want to see video on Web sites and sample the new emerging video applications, then network transmission rates of terabits are required. With a transmission rate of one Tbps, it is possible to transmit 20 million simultaneous 2-way phone calls or transmit the text from 300 years–worth of daily newspapers per second.

In addition to this explosion in consumer demand for bandwidth, many service providers are coping with fiber exhaust in their networks. Today, many operators are

nearing one hundred–percent capacity utilization across significant portions of their networks. Another problem for operators is the challenge of deploying and integrating diverse technologies in one physical infrastructure. Customer demands and competitive pressures mandate that carriers offer diverse services economically and deploy them over the embedded network. DWDM provides service providers an answer to that demand .

Use of DWDM allows providers to offer services such as e-mail, video, and multimedia carried as Internet protocol (IP) data over asynchronous transfer mode (ATM) and voice carried over SDH. Despite the fact that these format—IP, ATM, and SDH—provide unique bandwidth management capabilities, all three can be transported over the optical layer using DWDM. This unifying capability allows the service provider the flexibility to respond to customer demands over one network.

18.5 RESOLVING THE CAPACITY CRISIS

Faced with the challenges of increased service needs, fiber exhaust, and layered bandwidth management, service providers need options to provide an economical solution. One way to alleviate fiber exhaust is to lay more fiber; this will not be the most economical solution. However, laying new fiber will not necessarily enable the service provider to provide new services or utilize the bandwidth management capability of a unifying optical layer.

A second choice is to increase the bit rate using time division multiplexing (TDM), so that more bits (data) can be transmitted per second. Traditionally, this has been the industry method of choice (STM–1, STM –4, STM –16, etc.). However, when service providers use this approach exclusively, they must make the leap to the higher bit rate in one jump, having purchased more capacity than they initially need. Based on the SDH hierarchy, the next incremental step from 10 Gbps TDM is 40 Gbps—a quantum leap that may remain unutilized in the near future.

The telecommunications industry adopted the SDH standard to provide a standard synchronous optical hierarchy with sufficient flexibility to accommodate current and future digital signals. SDH accomplishes this by defining standard rates and formats and optical interfaces. For example, multiple electrical and optical signals are brought into a SDH terminal where they are terminated and multiplexed electrically before becoming part of the payload of an STM–1, the building block frame structure of the SDH hierarchy. The STM–1 payloads are then multiplexed to be sent out on the single fiber at a single rate: STM-4 to STM-16 to STM-64 and eventually to STM-256.

A synchronous mode of transmission means that the laser signals flowing through a fiber-optic system have been synchronized to an external clock. The resulting benefit is that data streams transmitting voice, data, and images through the fiber system flow in a steady, regulated manner so that each stream of light can readily be identified and easily extracted for delivery or routing.

18.6 CAPACITY EXPANSION AND FLEXIBILITY: DWDM

The third choice for service providers is dense wavelength division multiplexing (DWDM), which increases the capacity of embedded fiber by first assigning incoming optical signals to specific frequencies (wavelength, lambda) within a designated frequency band and then multiplexing the resulting signals out onto one fiber. Because incoming signals are never terminated in the optical layer, the interface can be bit-rate and format independent, allowing the service provider to integrate DWDM technology easily with existing equipment in the network while gaining access to the untapped capacity in the embedded fiber.

DWDM combines multiple optical signals so that they can be amplified as a group and transported over a single fiber to increase capacity. Each signal carried can be at a different rate and in a different format (SDH, ATM, data, etc.) For example, a DWDM network with a mix of SDH signals operating at 2.5 Gbps and 10 Gbps over a DWDM infrastructure can achieve capacities of over 40 Gbps. A system with DWDM can achieve all this gracefully while maintaining the same degree of system performance, reliability, and robustness as current transport systems. Today we are talking of DWDM terminals of up to 80 wavelengths of STM-16, a total of 200 Gbps, which is enough capacity to transmit 40,000 volumes of an encyclopedia in one second.

The technology that allows this high-speed, high-volume transmission is in the optical amplifier. Optical amplifiers operate in a specific band of the frequency spectrum, making it possible to boost light wave signals and thereby extend their reach without converting them back to electrical form. Demonstrations have been made of ultra wideband optical-fiber amplifiers that can boost light wave signals carrying over 100 channels (or wavelengths) of light. A network using such an amplifier could easily handle a terabit of information. At that rate, it would be possible to transmit all the world's TV channels at once or about half a million movies at the same time.

Consider a highway analogy where one fiber can be thought of as a multilane highway. Traditional TDM systems use a single lane of this highway and increase capacity by moving faster on this single lane. In optical networking, utilizing DWDM is analogous to accessing the unused lanes on the highway (increasing the number of wavelengths on the embedded fiber base) to gain access to an incredible amount of untapped capacity in the fiber. An additional benefit of optical networking is that the highway is blind to the type of traffic that travels on it. So, the vehicles on the highway can carry ATM packets, SDH, and IP.

18.7 CAPACITY EXPANSION POTENTIAL

By beginning with DWDM, service providers can establish a grow-as-you-go infrastructure, which allows them to add current and next-generation TDM systems for virtually endless capacity expansion. DWDM also gives service providers the flexibility

to expand capacity in any portion of their networks—an advantage no other technology can offer. Carriers can address specific problem areas that are congested because of high capacity demands. This is especially helpful where multiple rings intersect between two nodes, resulting in fiber exhaust.

Service providers searching for new and creative ways to generate revenue while fully meeting the varying needs of their customers can benefit from a DWDM infrastructure as well. By partitioning and maintaining different dedicated wavelengths for different customers, for example, service providers can lease individual wavelengths—as opposed to an entire fiber—to their high-use business customers.

Compared with repeater-based applications, a DWDM infrastructure also increases the distances between network elements—a huge benefit for long-distance service providers looking to reduce their initial network investments significantly. The fiber-optic amplifier component of the DWDM system enables a service provider to save costs by taking in and amplifying optical signals without converting them to electrical signals. Furthermore, DWDM allows service providers to do it on a broad range of wavelengths in the 1.55µm region. For example, with a DWDM system multiplexing up to 16 wavelengths on a single fiber, carriers can decrease the number of amplifiers by a factor of 16 at each regenerator site. Using fewer regenerators in long-distance networks results in fewer interruptions and improved efficiency.

18.8 THE OPTICAL LAYER AS THE UNIFYING LAYER

Aside from the enormous capacity gained through optical networking, the optical layer provides the only means for carriers to integrate the diverse technologies of their existing networks into one physical infrastructure. DWDM systems are bit-rate and format independent and can accept any combination of interface rates (e.g., synchronous, asynchronous, STM-1, STM-4, STM-16 etc) on the same fiber at the same time. If a carrier operates both ATM and SDH networks, the ATM signal does not have to be multiplexed up to the SDH rate to be carried on the DWDM network. Because the optical layer carries signals without any additional multiplexing, carriers can quickly introduce ATM or IP without deploying an overlay network.

But DWDM is just the first step on the road to full optical networking and the realization of the optical layer. The concept of an all-optical network implies that the service provider will have optical access to traffic at various nodes in the network, much like the SDH layer for SDH traffic. Optical wave-length add/drop (OADM) offers that capability, where wavelengths are added or dropped to or from a fiber, without requiring a SDH terminal. But ultimate bandwidth management flexibility will come with a cross-connect capability on the optical layer. Combined with OADM and DWDM, the optical cross-connect (OXC) will offer service providers the ability to create a flexible, high-capacity, efficient optical network with full optical bandwidth management.

18.9 KEY DWDM SYSTEM CHARACTERISTICS

There are certain key characteristics of acceptable and optimal DWDM systems. These characteristics should be in place for any DWDM system in order for carriers to realize the full potential of this technology. The following questions help determine whether a given DWDM system is satisfactory.

- Well-engineered DWDM systems offer component reliability, system availability, and system margin.
- An optical amplifier has two key elements: the optical fiber that is doped with the element erbium and the amplifier. When a pump laser is used to energize the erbium with light at a specific wavelength, the erbium acts as a gain medium that amplifies the incoming optical signal. If a connector is used rather than a splice, slight amounts of dirt on the surface may cause the connector to become damaged.
- Automatic adjustment of the optical amplifiers when channels are added or removed achieves optimal system performance. This is important because if there is just one channel on the system with high power, degradation in performance through self-phase modulation can occur. On the other hand, too little power results in not enough gain from the amplifier.
- In the 1530- to 1565-nm range, silica-based optical amplifiers with filters and fluoride-based optical amplifiers perform equally well. However, fluoride-based optical amplifiers are intrinsically more costly to implement.

It is possible to upgrade the channel capacity or wavelengths. However, for this they need either more power or additional signal-to-noise margin. For example, each time providers double the number of channels or the bit rate, 3 dB of additional signal-to-noise margin is needed.

18.10 VARIETIES OF WDM

Early WDM systems transported two or four wavelengths that were widely spaced. WDM and the "follow-on" technologies of CWDM and DWDM have evolved well beyond this early limitation.

18.10.1 WDM

Traditional, passive WDM systems are wide-spread with 2, 4, 8, 12, and 16 channel counts being the normal deployments. This technique usually has a distance limitation of less than 100 km.

18.10.2 CWDM

Today, coarse WDM (CWDM) typically uses 20-nm spacing (3000 GHz) of up to 18 channels. The CWDM Recommendation ITU-T G.694.2 provides a grid of wavelengths for target distances up to about 50 km on single mode fibers as specified in ITU-T Recommendations G.652, G.653 and G.655. The CWDM grid is made up of 18 wavelengths defined within the range 1270 nm to 1610 nm spaced by 20 nm.

18.10.3 DWDM

Dense WDM common spacing may be 200, 100, 50, or 25 GHz with channel count reaching up to 128 or more channels at distances of several thousand kilometers with amplification and regeneration along such a route.

18.11 DWDM SYSTEM FUNCTION

DWDM stands for ***D**ense **W**avelength **D**ivision **M**ultiplexing*, an optical technology used to increase Band width over existing fiber optic backbones. Dense wavelength division multiplexing systems allow many discrete transports channels by combining and transmitting multiple signals simultaneously at different wavelengths on the same fiber. In effect, one fiber is transformed into multiple virtual fibers. So, if you were to multiplex 32 STM-16 signals into one fiber, you would increase the carrying capacity of that fiber from 2.5 Gb/s to 80 Gb/s. Currently, because of DWDM, single fibers have been able to transmit data at speeds up to 400Gb/s.

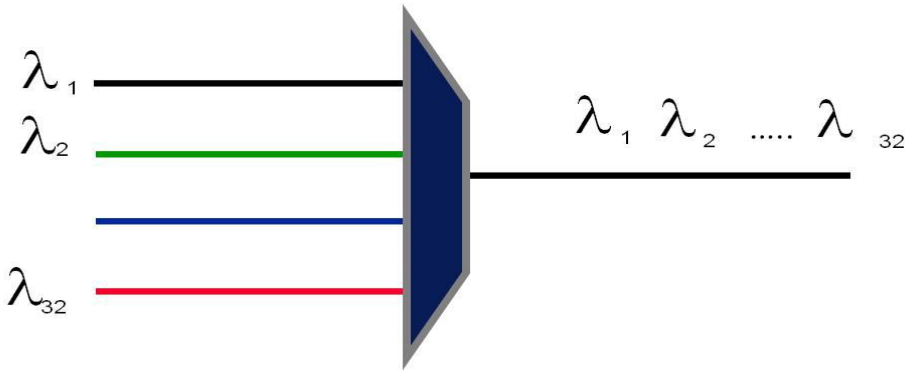


Figure 109: **Block Diagram of a DWDM System**

A key advantage to DWDM is that it's protocol and bit rate-independent. DWDM-based networks can transmit data in SDH, IP, ATM and Ethernet etc. Therefore, DWDM-based networks can carry different types of traffic at different speeds over an optical channel. DWDM is a core technology in an optical transport network. Dense WDM common spacing may be 200, 100, 50, or 25 GHz with channel count reaching up to 128 or more channels at distances of several thousand kilometers with amplification and regeneration along such a route.

The concepts of optical fiber transmission, loss control, packet switching, network topology and synchronization play a major role in deciding the throughput of the network.

18.12 TRANSMISSION WINDOWS

Today, usually the second transmission window (around 1300 nm) and the third and fourth transmission windows from 1530 to 1565 nm (also called conventional band) and from 1565 to 1620 nm (also called Long Band) are used. Technological reasons limit DWDM applications at the moment to the third and fourth window.

The losses caused by the physical effects on the signal due by the type of materials used to produce fibres limit the usable wavelengths to between 1280 nm and 1650 nm. Within this usable range the techniques used to produce the fibres can cause particular wavelengths to have more loss so we avoid the use of these wavelengths as well.

18.13 DWDM SYSTEM COMPONENTS

Figure116 shows an optical network using DWDM techniques that consists of five main components:

18.13.1 Transmitter (Transmit Transponder):

- Changes electrical bits to optical pulses

- Is frequency specific

- Uses a narrowband laser to generate the optical pulse

18.13.2 Multiplexer/ Demultiplexer:

- Combines/separates discrete wavelengths

18.13.3 Amplifier:

- Pre-amplifier boosts signal pulses at the receive side

- Post-amplifier boosts signal pulses at the transmit side (post amplifier) and on the receive side (preamplifier)

- In line amplifiers (ILA) are placed at different distances from the source to provide recovery of the signal before it is degraded by loss.

- EDFA (Eribium Doped Fiber Amplifier) is the most popular amplifier.

18.13.4 Optical Fiber (Media):

- Transmission media to carry optical pulses

- Many different kinds of fiber are used

- Often deployed in sheaths of 144–256 fibers

18.13.5 Receiver (receive transponder)

- Changes optical pulses back to electrical bits

- Uses wideband laser to provide the optical pulse

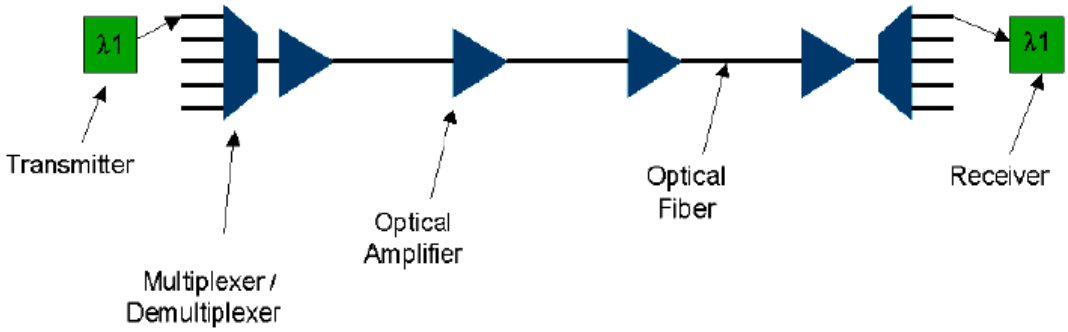


Figure 110: **DWDM System Components**

18.14 BENEFITS OF DWDM

- Increases bandwidth (speed and distance)
- Does not require replacement or upgrade their existing legacy systems
- Provides "next generation" technologies to meet growing data needs
- Less costly in the long run because increased fiber capacity is automatically available; don't have to upgrade all the time

18.15 CONCLUSION

DWDM promises to solve the "fiber exhaust" problem and is expected to be the central technology in the all-optical networks of the future. This increase means that the incoming optical signals are assigned to specific wavelengths within a designated frequency band, then multiplexed onto one fiber. This process allows for multiple video, audio, and data channels to be transmitted over one fiber while maintaining system performance and enhancing transport systems. This technology responds to the growing need for efficient and capable data transmission by working with different formats, such as SONET/SDH, while increasing bandwidth.

19 CONCEPT OF ONE NETWORK (CENTRALIZED NOC FOR CFA)

19.1 LEARNING OBJECTIVES

- Concept and requirement of One Network
- Activities involved in one network concept
- Implementation of one network program
- Learn about the network and partner team management

19.2 INTRODUCTION TO ONE NETWORK

- The activities related to network management and customer management are being done currently at the exchange / equipment location level. Customer service management is generally done through indoor staff stations at main exchange locations and outdoor takes care of last mile activities. The commercial activities related to partner (cluster, FTTH) management are being done in a decentralized manner.

- With the change in technology and management methodologies, it is very much desired that 24/7 network management is done through a centralized location for first level monitoring and corrective action required for the operational excellence. Wherever physical presence of staff is required for change of network card etc., there should be common staff at site to manage technical equipment, power plan, electrical infrastructure, etc.

- One network program was started by BSNL on 16-12-2020

- One network is Centralized NOC (Network operations center) for CFA (Consumer Fixed Assets)

19.3 ACTIVITIES IN ONE NETWORK

Following Activities are proposed for centralized network/customer/partner management.

(A) Network Management

- FTTH /OLT Management.
- OMCR- BTS Monitoring
- OF Route Patroller Monitoring
- NIB Network Elements Management (BNG/RPR/OCLAN/MNGPAN /Facebook Cache Server/Google Cache Server) Monitoring and Management

(B) Partner Management

A Centralized Group for Partner Support (CGPS) shall operate performing the following separate activities for the cluster / FTTH partners.

- Partner on boarding including all paper work for signing, creation of user id/login to various IT systems like FMS, DKYC, CDR systems, E-pay system, Wallet, etc.
- Monthly settlement of revenue share through ERP and Wallet.
- Exchange of all information related to sales and market activities.
- Common toll free number opened by ITPC is 18005991001 (created by Bangalore Telecom District for partner management activities) shall be mapped with the telephone number at respective BA level CGPS.
- A telephonic PIN (T-Pin) shall be issued to all partners so that call from the partners can be routed to the respective BA P-CSG.
- For this every BA will have its own 3-digit PIN and its corresponding destination number/ line hunting group.

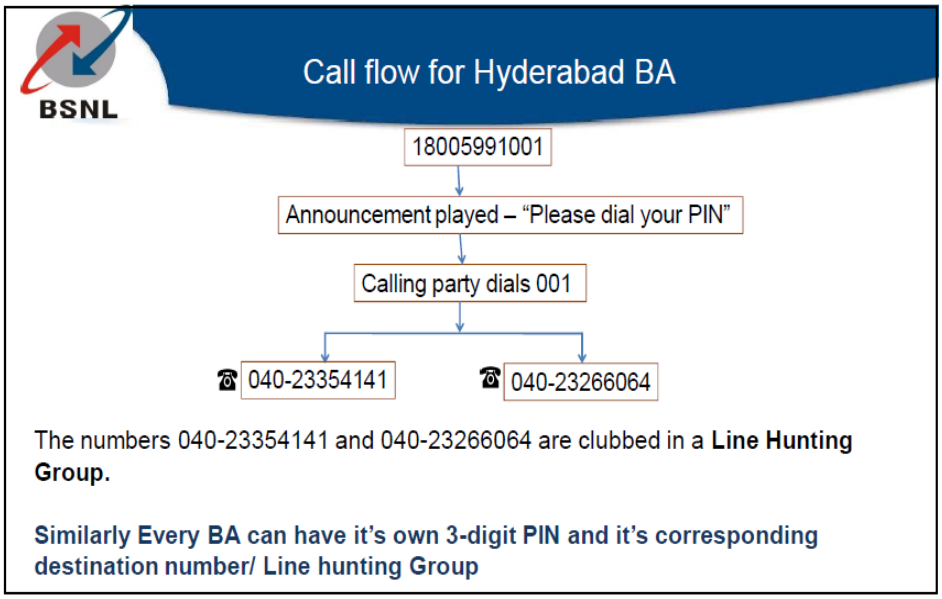


Figure 111: **Call flow for BA**

19.4 FTTH MANAGEMENT (BSNL OLT/TIP OLT/BBNL OLT)

- FTTH OLT Management (EMS)
- FTTH Soft Switch Management (Voice Creation)
- FTTH Lead Management.
- FTTH Fault Management.

- FTTH CAF Approval.
- CDR activities with respect to FTTH.
- FTTH TIP support.

19.5 OMCR ACTIVITIES

- BTS Monitoring (2G/3G/4G) and Reporting
- TRE/Combiner HW Reset
- Partial Fault Monitoring
- Attending calls from field persons
- BTS External Alarm Monitoring

19.6 OFC ROUTE PATROLLER MONITORING

- Patroller Monitoring and Reports.
- Updation of data for Patrollers and New OF route in Patroller Monitoring System.

- **NOC FOR ONE NETWORK**

NOC of ONE Network has terminals of OMCRs, FTTH, NIB, eMS, Softswitch, ROT, CPAN, CDR, ERP extended for operations, monitoring and control. It is equipped with large LED screens for display of status and health of the network.

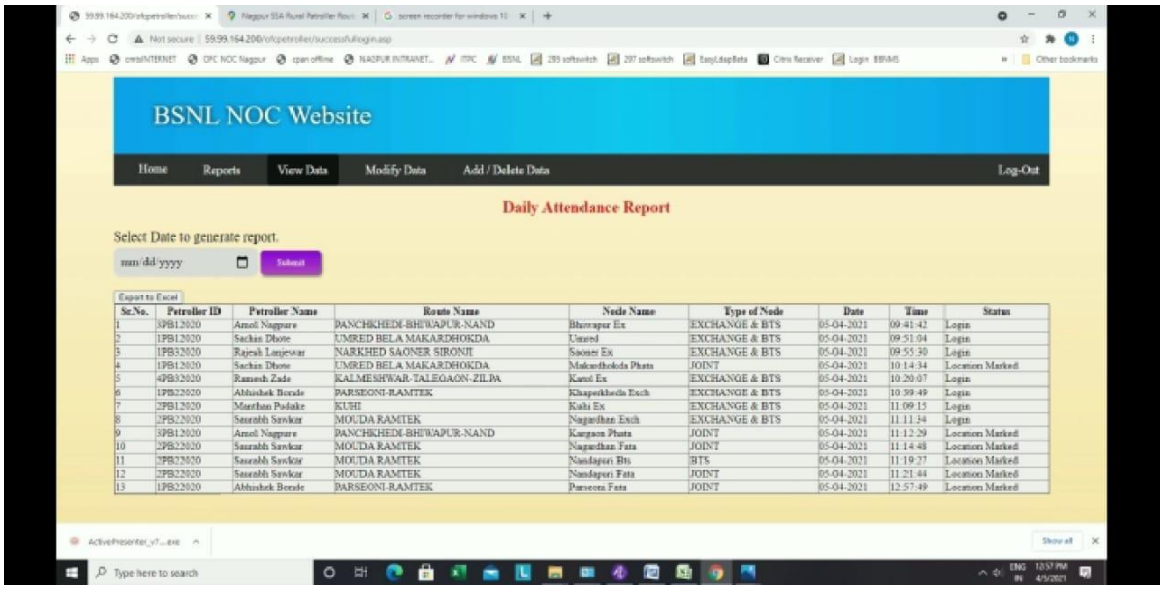


Figure 112: **BSNL NOC Website**

19.7 MORE ACTIVITIES PROPOSED IN ONE NETWORK

- Transmission system monitoring and management
- NGN-LMGs/DSLAMs/OLTs/Exchange Monitoring and management
- NOFN – OLT/ONT monitoring and management
- PRI & SIP Monitoring and Management
- LEASED CIRCUIT & MLLN Monitoring and Management (DXC/V-MUX/Circuits)
- CDR/FMS SYSTEM management (Central Router/Exchange Router/MLLN Circuits)
- Wi-Fi Hotspots- monitoring & Management
- High Bandwidth Circuit Monitoring & management
- MPLS Monitoring (Edge Router/Core Router/Super Core Router/Circuits)

19.8 NETWORK MANAGEMENT BA TEAM

BA Team wise size required for centralized NOC activities and partner support group is to be prepared in following format

(A) Network Management Team Details

Name	Designation	Monitoring on network elements (FTTH/OLT/BNG etc.)	Mobile No.	E-mail ID

(B) Partner Management Team Details

Name	Designation	CLUSTER FTTH	Mobile No.	E-mail ID

19.9 ONE NETWORK BA TEAM CASE STUDY OF MAHARASHTRA CIRCLE

Sl. No.	Name of circle	Name of BA	BA Type	Members in the centralized NOC team for network management	Members in the CGPS for the cluster/FTTH partner
1	MH	Ahmednagar	Category-B	12	6
2	MH	Amaravati	Category-C	8	4
3	MH	Aurangabad	Category-C	8	4
4	MH	Chandrapur	Category-C	8	4
5	MH	Goa	Category-C	8	4
6	MH	Jalgaon	Category-C	8	4
7	MH	Kalyan	Category-B	12	6
8	MH	Kolhapur	Category-B	12	6
9	MH	Nagpur	Category-C	8	4
10	MH	Nanded	Category-C	8	4
11	MH	Nashik	Category-C	8	4
12	MH	Pune	Category-A	16	8
13	MH	Satara	Category-C	8	4
14	MH	Solapur	Category-C	8	4

19.10 CONCLUSION

As the name suggest one network program is a drive to monitor all the network components at a centralize location with 24x7 watch on the entire level and provide first level of escalation. With the growing number of subscribers and network elements to cater to such huge subscriber base, it is necessary to monitor the entire network for seamless services round the clock. One Network program is an initiative towards the NOC based approach.

20 WI-FI AND CYBER SECURITY

20.1 LEARNING OBJECTIVES

- Benefits and disadvantages of Wi-Fi
- Wi-Fi standards
- Architecture
- Media access control
- Wi-Fi connections
- Wi-Fi security
- System vulnerabilities to attack
- Major security threats

20.2 INTRODUCTION

Wi-Fi is the wireless way to handle networking. It is also known as **802.11 networking**. The big advantage of Wi-Fi is its simplicity.

You can connect computers anywhere in your home or office without the need for wires. Thecomputers connect to the network using radio signals, and computers can be up to 100 feet or so apart.

20.2.1 A Simple Wi-Fi Network

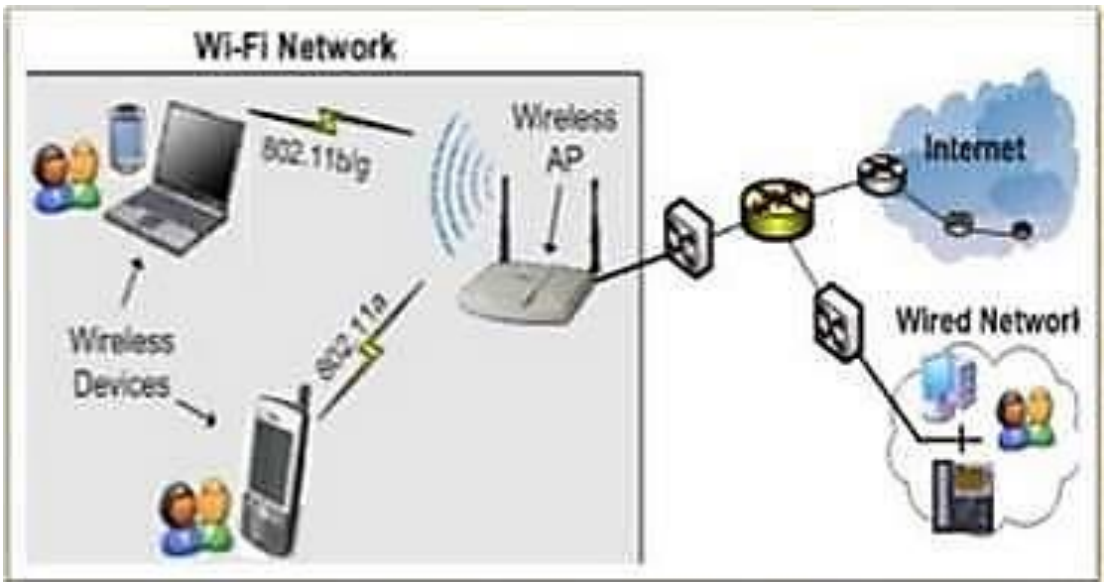


Figure 113: **A simple WIFI**

20.2.2 Wi-Fi Range

Regardless of which setup you use, once you turn yourWireless Access Point on, you will have a Wi-Fi hotspotin your house.In a typical home, this hotspot will provide coverage for about 100 feet (30.5 meters) in all directions, although walls and floors do cut down on the range.Even so, you should get good coverage throughout a typical home. For a large home, you can buy inexpensive signal boosters to increase the range of theHotspot.

20.3 ADDING WI-FI TO YOUR COMPUTER

Many new laptops already come with a Wi-Fi card built

It is also easy to add a Wi-Fi card to a laptop or a desktop PC.

Buy a suitable standard network card.

- For a laptop, this card is a PCMCIA
- For a desktop machine, buy a PCI card or USB type

Install the driver

20.4 BENEFITS & DISADVANTAGES

20.4.1 Benefits Of Wi-Fi

- Mobility
- Compatibility with IP networks
- High speed data
- Unlicensed frequencies
- Security
- Easy and fast installation
- Scalability
- Low cost

20.4.2 Disadvantages Of Wi-Fi

- Generates radiations which can harm the human health
- We must disconnect the Wi-Fi connection whenever not using
- Not very long distance communication
- Compared to wired connection, still costly

20.5 WI-FI STANDARDS

- Standards are mutually agreed upon rules adopted by the industry on how the

wireless networks operate.

- The core protocols are listed in the 802.11 standards, which was originally available in 1997
- There are a couple of standards that describe Wi-Fi. All of them are part of the 802.11 suite.

Network standard	Maximum Speed (Mbps)	Range (feet)	Frequency (GHz)	Power drain	Cost
802.11b	11	100-150	2.4	Moderate	Low
802.11a	54	60-100	5	High	High
802.11g	54	150-250	2.4	Moderate	Moderate
802.11n	200	Up to 300 feet	2.4 & 5	Moderate	Moderate

Figure 114: **IEEE Standards**

20.5.1 IEEE 802.11 Suite

- WiFi radios that work with the 802.11b and 802.11g standards transmit at 2.4 GHz, while those that complywith the 802.11a standard transmit at 5 GHz.
- Normal walkie-talkies normally operate at 49 MHz. The higher frequency allows higher data rates.
- WiFi radios use much more efficient coding techniques (process of converting 0's and 1's into efficient radio signals) that also contribute to the much higher data rates.
- The radios used for WiFi have the ability to changefrequencies
- For example, 802.11b cards can transmit directly onany of three bands, or they can split the available radio bandwidth into dozens of channels and **frequency hop** rapidly between them.

- The advantage of frequency hopping is that it is much more immune to interference and can allow dozens of WiFi cards to talk simultaneously without interfering with each other.

802.11b: First to reach the marketplace. It is the slowest and least expensive of the three. 802.11b transmits at 2.4 GHz and go up to 11Mbps.

802.11a: Was next. It operates at 5 GHz and can handle up to 54 Mbps.

802.11g: Mix of both worlds b & g. It operates at 2.4Ghz (giving it the cost advantage of 802.11b) but it has the 54 megabits per second speed of 802.11a. It is also backward compatible to 802.11b.

802.11ac : Backward compatible with 802.11n & its predecessors, maximum of 450 megabits per second on a single stream, sometimes called **5G WiFi** because of its frequency band, sometimes **Gigabit WiFi** because of its potential to exceed a gigabit per second on multiple streams

20.6 WI-FI BACKGROUND

1990 : 802.11 development started by IEEE

The aim was to develop a standards for medium access control (MAC) and physical layer (PHY)

1997 : First version of 802.11 standard was ratified

First version delivered 1Mb/s and 2Mb/s data rates

1999 : 802.11a and 802.11b amendments were released Data rates improved to 5.5Mb/s and 11Mb/s at 2.4GHz (802.11) Wired Equivalent Privacy (WEP) introduced

5GHz operation with OFDM modulation at 54Mb/s (802.11a)

2001 : FCC approved the use of OFDM at 2.4GHz

2003 : OFDM modulation at 54Mb/s at 2.4GHz (802.11g)

2009 : 801.11n amendment were ratified

PHY relies heavily on multiple-input multiple-output (MIMO) technology

Can use both 2.4Ghz and 5Ghz at the same time

Throughput increased even up to 600Mbps

2009 : Bluetooth 3.0 + HS

802.11 selected as the Bluetooth high speed channel

2009 : Wi-Fi direct specification introduced

2011 : 802.11ac development started

More throughput with wider bandwidth, more MIMO streams and wider 256-QAM modulation. Provides 500-1000Mbps throughput

20.7 802.11 ARCHITECTURE

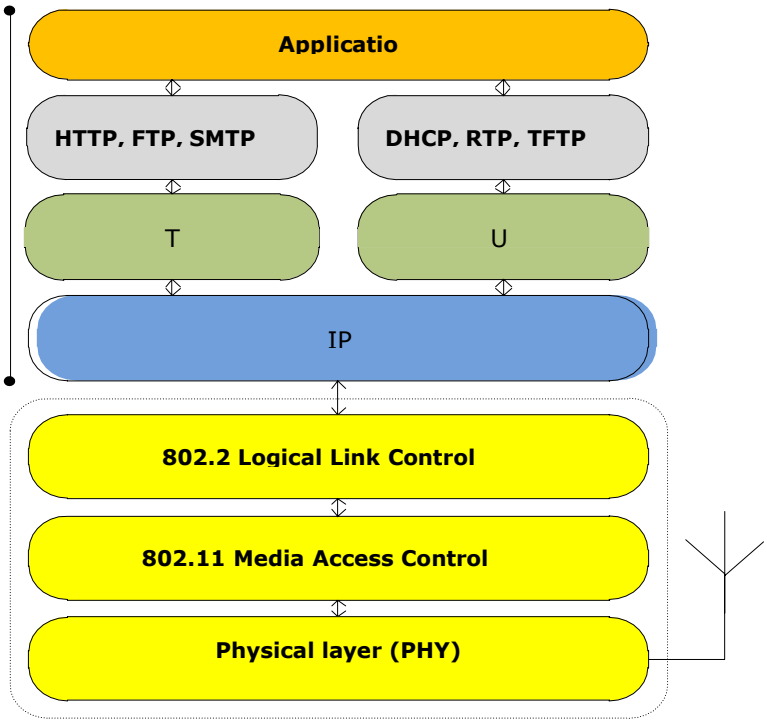


Figure 115: **802.11 architecture**

Physical Layer

- 2.4 GHz and/or 5GHz transciever Industrial Scientific Medical (ISM) band License free

Spread spectrum technology

- FHSS, DSSS and OFDM modulations

FHSS (Frequency Hopping Spread Spectrum)

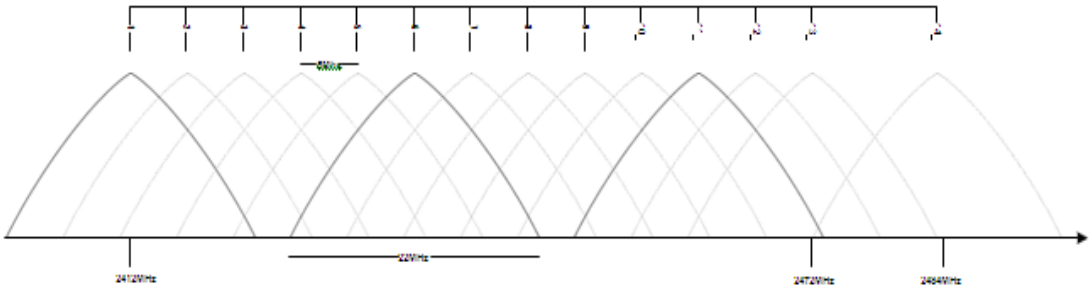
- Bandwidth divided into 75 1MHz channels
- Data throughput limited to 2Mbps because of hopping overhead and FCC regulations (1 Mhz channel bandwidth)

DSSS (Direct Sequency Spread Spectrum)

- Bandwidth divided into 14 22MHz channelsChannels overlap partially

OFDM (Orthogonal Frequecy-Division Multiplexing)

- 20 or 40MHz bandwidth
- Uses several non-overlapping channelsChannels overlap partially



Europe : channels 1-13
USA : channels 1-11
Japan : channels 1-14

Figure 116: **Wi-Fi Physical Layer Channels**

Standard	Frequency	Bandwidth (MHz)	Symbol rate (Mb/s)	MIMO streams	Modulation
802.11	2.4GHz	20	1, 2	1	DSSS, FHSS
802.11a	5Ghz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM
802.11b	2.4GHz	20	5.5,11	1	DSSS
802.11g	2.4GHz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS
802.11n	2.4/5GHz	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM
		40	15, 30, 34, 60, 90, 120, 135, 150		

Table 7. Comparison between various standards

20.8 802.11 MEDIA ACCESS CONTROL (MAC)

- Manages and maintains communications between 802.11 stations and clients
- Coordinates access to shared radio channels Uses CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) algorithm to access the media
- Similar to Bluetooth Link Layer

- Because of the shared media operation, all Wi-Fi networksare half duplex.
- All Wi-Fi networks are contention-based TDD systems, where the access point and the mobile stations all vie for use of the same channel.
- There are equipment vendors who market WiFi mesh configurations, but those implementations incorporatetechnologies that are not defined in the standards.

Function	Explanation
Scanning	Scanning of access points. Both active (probe) and passive (beacon) scanning are provided by the standard.
Authentication	Authentication is the process of proving identity between the client and the access point.
Association	Once authenticated, the client must associate with the access point before sending dataframes.
Encryption	Encryption of payload
RTS/CTS	The optional request-to send and clear-to-send (RTS/CTS) function allows the access point to control use of the medium for stations activating RTS/CTS.
Power SaveMode	The power save mode enables the user to turn on or off enables the radio.
Fragmentation	The fragmentation function enables an 802.11 station to divide data packets into smaller frames.

20.9 LOGICAL LINK CONTROL (LLC)

The LLC provides end-to-end link control over 802.11-based wireless LAN

LLC services:

Unacknowledged connectionless service

- Higher layers must take care of error and flow control mechanisms
- Peer-to-peer, multicast and broadcast communication

Connection-oriented service

- Error and flow control
- Peer-to-peer communication

Acknowledged connectionless service

- Flow and error control with stop-and wait ARQ
- Peer-to-peer, multicast and broadcast communication

20.10 WI-FI CONNECTIONS

- Connection (Logical) is the mutual agreement between two ports to have a communication.
- Wi-Fi networks can be of BSS and ESS types
- Two Wi-Fi devices can have mainly two types ofconnections.
  - Ad-hoc connection (Peer-to-Peer connection)
  - Infrastructure connection (AP Connection)
  -

Ad-hoc Mode

- Essentially a peer-to-peer(also called work group) model.
- Ad Hoc connections can be used to share information directly between devices. This mode is also useful for establishing a network where wireless infrastructure does not exist.

Some uses,

- Synchronize data between devices.
- Retrieve multimedia files from one device and "play" them on another device.
- Print from a computer to a printer without wires.
- There are many applications of ad hoc networking in the military and in specialized networks

Infrastructure Mode

- Essentially a Client/Server model
- Infrastructure mode connection can be used to share information from one Wi-Fi client to AP.
- Many Wi-Fi clients can access an AP at a time
- Normally used to access internet.

Basic Service Set (BSS)

- A set of stations controlled by a single "Coordination Function"
- Typically uses an Access Point (AP)
- All mobile stations must be accessible by theaccess point of the infrastructureBSS
    - In the infrastructure network, stations must associate with the access point in order to getaccess to network services

Independent Basic Service Set (IBSS)

A BSS without an Access-Point is basically ad-hoc networking

Extended Service Set (ESS)

A set of one or more Basic Service Sets interconnected by a Distribution System (DS). Traffic always flows via Access-Point

Distribution System (DS):

A system to interconnect two or more BSS

Typically wired Ethernet

Could be also wireless like 802.11, WiMax,3G/4G etc.

AP – client services:

Authentication/ De-authentication: open, shared key or WPS

Privacy : WEP, WPA or WPA2

Distribution System services:

Association: maps the client into the distribution system via access point

Disassociation: release of association

Distribution: used to deliver MAC frames across the distribution system

Integration: enables delivery of MAC frames between DS and non 802.11

Re-association: transition of association from one access point to an other

20.11 WI-FI SECURITY

WiFi hotspots can be open or secure.

If a hotspot is open, then anyone with aWiFi card can access the hotspot.

If it is secure, then the user needs to know a Security key

20.12 WI-FI SECURITY FEATURES

The 802.11 provides the following security features

Association - Client needs to associate with the Access Point

Authentication- Authentication is either open, shared key or WPS

Access control (MAC Filter)- Access Point can decide which clients are allowed to associate based on MAC addressTrivial to spoof MAC address

20.13 WI-FI SECURITY TYPES

20.13.1 Encryption

Wired Equivalent Privacy (WEP) - (insecure)

Wireless Protected Access (WPA) - (insecure)

Wireless Protected Access 2 (WPA2) –(Secure)

Data integrity

Data can not be modified on-the-fly. Quarantined by Encryption.

Data confidentiality

No eavesdropping with decryption of data. Quarantined by encryption.

20.13.2 WEP (Wired Equivalent Privacy)

This encryption standard was the original encryption standard forwireless.

Security issues known since 2001, can be cracked in <1minute

WEP has two variations: 64-bit encryption and 128-bit encryption

64-bit encryption was the original standard but was found to be easily broken.

128-bit encryption is more secure and is what most people use if they enable WEP.

For a casual user, any hotspot that is using WEP is inaccessible unless you know this WEP key.

20.13.3 WPA (Wi-Fi Protected Access)

WPA is the successor to WEP

WPA uses TKIP for encryption, some routers also supportAES.

Security issues known since 2008 in TKIP, consideredunsecure

Latest version of WPA is WPA2 (Uses TKIP or AES)

20.13.4 Wireless Protected Access 2 (WPA2)

WPA2 is a Wi-Fi Alliance branded version of the final 802.11i standard. The primary enhancement over WPA is the inclusion of the AES- algorithm as a mandatory feature.

The CCMP/AES algorithm is considered secure, given a good enough password

WPA2 Personal (WPA2-PSK): Uses a password, common.

WPA2 Enterprise (WPA2-RADIUS): Certificates on server

Note: Wi-Fi Alliance will mandate Wi-Fi CERTIFIED products only to support WPA2 AES

20.14 SETTING UP WI-FI HOTSPOT AT HOME

If you already have several computers hooked together on an Ethernet network and want to add a wireless hotspot to the mix,you can purchase a **Wireless Access Point** and plug it into the Ethernet network.

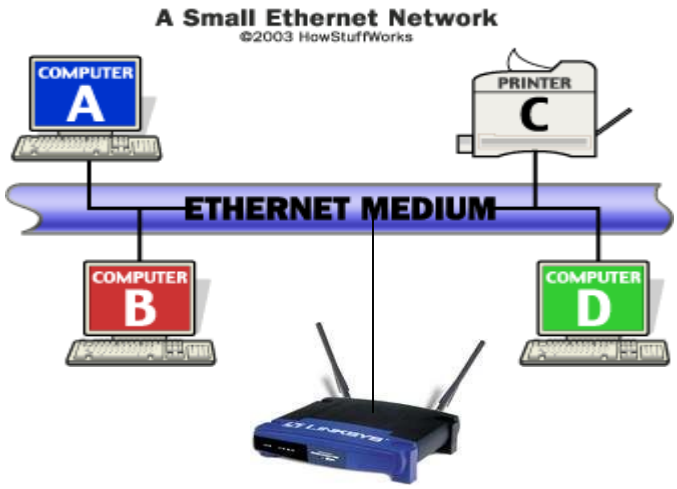


Figure 117: **Wireless Access Point**

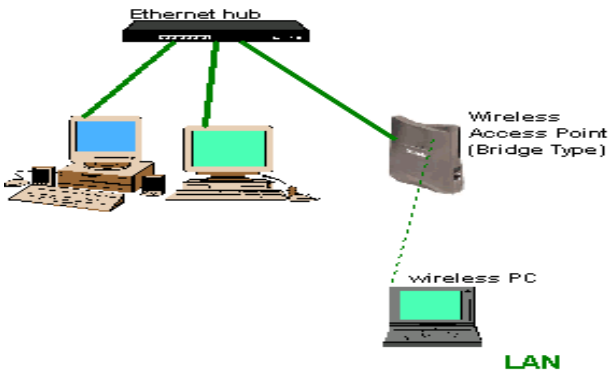


Figure 118: **Different types of IProuting**

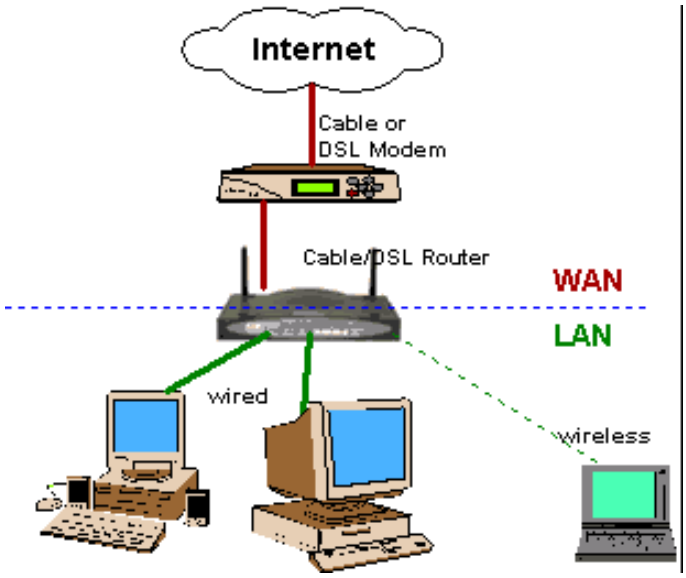


Figure 119: **Alternate Setup using a Wireless Router**

If you are setting up a network in your home forthe first time, or if you are upgrading, you can buy a Wireless Access Point Router.

This is a single box that contains:

1) a port to connect to your cable modem or DSL modem,
2) a router,
3) an Ethernet hub,
4) a firewall and
5) a wireless access point.

You can connect the computers in your home to this box either with traditional Ethernet cables or with wireless cards.

20.15 CONFIGURING A HOTSPOT

Most wireless access points come with defaultvalues built-in.

Once you plug them in, they start working withthese default values.

However, you may want to change things.

You normally get to set three things on youraccess point.

20.15.1 Things To Configure In A Hotspot

The SSID -- Service Set IDentifier is a sequence of characters that uniquely names a WLAN.

The channel – the radio link used by access point/router to communicate to wireless devices. Normally it will default to channel 6.

However, if a nearby neighbor is also using an access pointand it is set to channel 6, there can be interference. Chooseany other channel between 1 and 11.

The WEP or WPA key – Normally select WPA

Access points come with simple instructions for changing these three values. Normally you do it with a Web browser. Once it is configured properly, you can use your new hotspot to access the Internet from anywhere in your home. Additionally you can configure ACL (MACFilter)

IEEE 802.11ac

- **The next generation after IEEE 802.11n -** 433Mbit/s - 1Gbit/s data rates (not throughput)
- **Throughput through wider channels -** 80MHz and 160MHz
- **More dense modulation -** 256-QAM

20.16 WI-FI ALLIANCE

- An open, non-profit organization responsible of : Wi-Fi standards development, marketing, Wi-Fi certification etc.
- Wi-Fi Alliance developed standards: WPA, WPA2, Wi-Fi Direct etc.
- Formed originally to resolve the interoperability issues between different manufacturers' 802.11 devices.Similar organization to Bluetooth SIG

20.17 CYBER SECURITY

In the age of Information Revolution, the management of information and its security is the key concern for all organizations and nations. For sharing of information among the intended users, the systems have to be networked. With networking, the risk of unauthorized use and attack has taken major attention of managers. Networks and Information are subject to various types of attacks, various products are available in the market for securing the systems. But it needs the thorough understanding of the various issues involved and proper implementation. In the cyber world, the current state of the practice regarding the technical ability to track and trace Internet-based attacks is

primitive at best. Sophisticated attacks can be almost impossible to trace to their true source using current practices. The anonymity enjoyed by today's cyber attackers poses a grave threat to the global information society, the progress of an information based international economy, and the advancement of global collaboration and cooperation in all areas of human endeavor. The domestic and international implication of an increasingly critical societal dependence on the Internet makes necessary the ability to deter, or otherwise minimize, the effects of cyber-attacks.

Home computers are typically not very secure and are easy to break-in. When combined with high-speed Internet connections that are always turned on, intruders can quickly find and then attack home computers. While intruders also attack home computers connected to the Internet through dial-in connections, high-speed connections (cable modems and DSL modems) are a favorite target. There may not be important data stored on the home computers but they are targeted by the intruders for launching attack against other computer systems.

What is cyberspace?

It is an electronic world created by interconnected networks of information technology and the information on those networks.

What is cyber security?

Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

Cyber threats

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four: cyber espionage, cyber warfare, cyberterrorism, and cyber crime

1. **Cyber espionage:** Intelligence gathering and data theft. Examples of this were Titan Rain and Moonlight Maze
2. **Cyber warfare:** It involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks.
3. **Cyber terrorism**: It is premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence
4. **Cybercrime:** It is any criminal activity that involves a computer, networked device or a network.

20.17.1 Information Security

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected' [BS ISO 27002:2005]

Information can be created, stored, destroyed, processed, transmitted or used; whatever forms the information takes or means by which it is shared or stored, it should always be appropriately protected. [BS ISO 27002:2005]

Information security means to make the shared information always available to authentic users without loss and assuring confidentiality. As well Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information security is concerned with the CIA of data regardless of the form the data may take: electronic, print, or other forms.

Preservation of CIA of information; in addition, other properties such as authenticity, accountability, non-repudiation & reliability can also be involved. [ISO/IEC 17799:2005]

20.17.2 Importance Of Information Security

a. Regulatory Compliance –
IT (Amendment) Act 2008 and IT Act 2000

b. Security Risk Management
Reducing exposures to technology threats

Preventing computer-related frauds

Enforce policies and improve audit capability

c. Reducing Operational Costs
Reducing cost of unexpected security events

Reducing losses from frauds and security failures

d. Consequences
Loss of competitive advantage

Service interruption

Embarrassing media coverage

Legal penalties

20.17.3 Information Security Components

Information Security Components: or Qualities are (CIA)

a. Confidentiality - Preventing disclosure of information to unauthorized individuals or systems
b. Integrity - Data shall not modify without authorization.
c. Availability - Information must be available when it is needed

Figure 120: **Security Component CIA Model**

20.17.4 Sources Of Information For Intruders

Intruder can hack your Information by using techniques such as:-

Dumpster diving –Waste Baskets searching, Thrown papers, Scrapped Hard Disks

Social Engineering- Talent hack, Help Desk persons, Tech support persons Administrative support persons, Reception staff, Retired Employees, Vendors Contractors, Partners etc may give out Information Knowingly or unknowingly.

Information System- Electronically, Email Accounts (Default usernames and Passwords)

Networked PC's (Using Virus activity) ,web pages(biodatas)

20.18 TYPES OF ATTACKS ON INFORMATION SYSTEM

Malicious Code Attacks

Known Vulnerabilities

Configuration Errors

20.18.1 Indication Of Infections

Poor System Performance

Crashing of Applications

Abnormal System Behavior

Unknown Services are running

Change in file extension or contents

Automatic shutdown of System

System Not Shutting Down

Hard Disk is Busy

20.18.2 Systems Vulnerablities To Attack

Information system becomes vulnerable to attack due to following reasons
Use of Default User Accounts and Password

Remote Access Not Disabled

Logging and Audit Disabled

No proper Access Controls on Files

Non Availability of Updated Antivirus and Firewall

Un-necessary Services running

20.18.3 Achieving Security By Monitoring

A lot can be observed by just watching & paying attention to what you can see & measure.

Monitor for any changes in configuration of 'High risk' devices

Monitor failed login attempts, unusual traffic, changes to the Firewall, access grants to firewall, connection setups through Firewalls

Monitor server logs

20.18.4 Security Implementation Levels

OS/NOS level

Keep OS updated with service packs (OS Release)

Install security patches for OS

Install up-to-date antivirus software

Disable remote access

Harden OS by turning off unnecessary services and features

20.18.5 Application Levels

Keep Application Package Updated

Install Security patches for Application Packages

Do not Install Programs of unknown origin

Take precautions while using emails

Secure web Browsers

20.18.6 RDBMS Level

User Management

Managing Allocation of Resources to Users

Password Policy

Backup and Recovery

Auditing

20.18.7 Network Level

Use of Firewalls to Monitor and control Network Traffic.

Monitor for any changes in Configuration of 'High risk' Devices eg firewalls.

Monitor Failed Login Attempts

Monitor Server Logs

20.19 MAJOR SECURITY THREATS

High profile virus attacks in the recent past have forced a few businesses to shut down connections to the Internet. New viruses and malicious code are used to commit cybercrime and criminal acts. It pays to be aware of the various security threats.

- Viruses
- Worms
- Trojan Horses
- Malware
- Adware
- Spam

20.19.1 Viruses

A virus is a small piece of software (code) that piggybacks on real programs, O.S. or e-mails. Virus is loaded onto your computer without your knowledge and runs against your

wishes. Each time a program runs the virus gets executed.

Type of Viruses

a. Executable Viruses
b. Boot sector viruses
c. E-mail viruses

Executable Viruses

Traditional Viruses

Pieces of code attached to a legitimate program

Run when the legitimate program gets executed

Loads itself into memory &looks around to see if it can find any other programs on disk

E-mail Viruses

Moves around in e-mail messages

Replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book

Example: Melissa virus etc.

Some e-mail viruses don't even require a double-click, they launch when you view the infected message in the preview pane of your e-mail software

Macro Viruses

Infect programming environments rather than OS or files.

Almost any application that has it's own macro programming environment
MS Office (Word, Excel, Access…)
Visual Basic
Application loads a file containing macro and executes the macro upon loading or runs it based on some application based trigger.

Melissa was really successful macro virus

Usually spread as an e-mail attachment

Most Damaging Viruses

Melissa Virus

Estimated financial damage-300 to 600 million dollars

Affected 15-20% of all business PCs

Spread via email

20.19.2 Worms

Network Worms are self replicating programs which spread all over the Internet at a very fast rate. They cause a huge bandwidth drain while propagating and sometimes bring even large networks down to their knees.

20.19.3 Difference Between Worm & Virus

The differ in the method of attachment; rather than attaching to a file like a virus a worm copies itself across the network without attachment.

All copies have the same functionality and generally lack any sort of synchronization among themselves.

Infects the environment rather than specific objects.

Morris Worm, WANK, CHRISTMA EXEC

20.19.4 The Life Cycle Of A Simple Worm

a. Scanning for a victim (Scan IP)
b. Exploiting the victim (a piece of code which provides “access” by utilizing some flaw on the victim computer)
c. Cloning itself onto the victim (copy of itself on the victim PC as FTP / HTTP server)
d. Running the clone to further spread infection (Make it a service, Add a registry entry, Clone starts spreading infection further)

20.19.5 Trojan Horses

Trojan is a type of malware that pretends to be something useful, helpful, or fun while actually causing harm or stealing data.

Trojans are often silently downloading other malware (e.g. spyware, adware, ransomware) on an infected device as well.

a. Trojan horses are dangerous programs that hide within other seemingly harmless programs.
b. Once they're installed, the program will infect other files throughout your system and potentially wreak havoc on your computer.
c. They can even send important information from your computer over the Internet to virus developer.
d. The developer can control your computer, slowing your system's activity or causing your machine to crash.
e. Used to remotely control windows

f. Categorized as RAT(Remote Administration tool)
g. Used for stealing credit card information
h. Works on most of the operating systems
i. Worms and Trojan horses are actually more common today than viruses.
j. Antivirus programs offer protection against all viruses, worms, and

20.19.6 Malware

The word "malware" comes from the term "MALicious softWARE." Malware is any software that infects and damages a computer system without the owner's knowledge or permission.

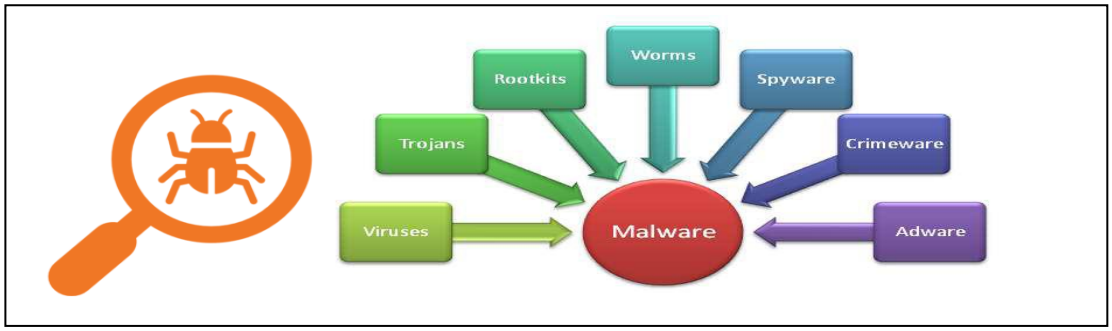


Figure 121: **Malware**

20.19.7 Adware

Adware is a type of malware that bombards you with endless ads and pop-up windows that could potentially be dangerous for your device. The best way to remove adware is to use an adware removal tool.

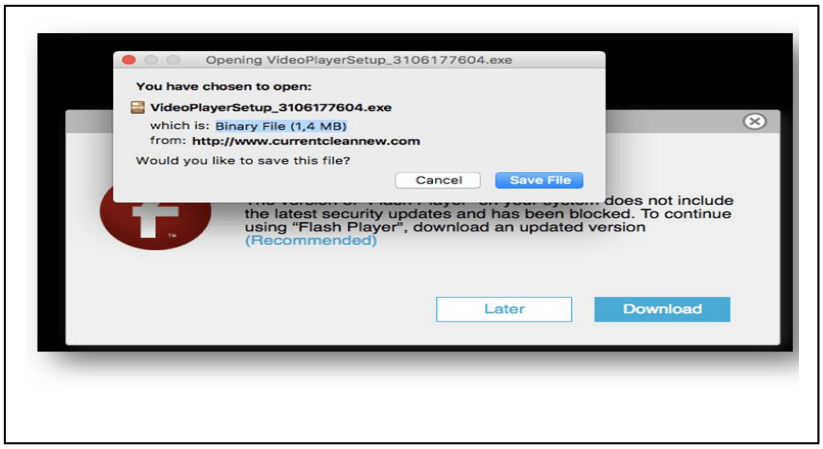


Figure 122: **Adware**

20.19.8 Spam

a. Spamming is the use of electronic messaging systems to send unsolicited messages (spam), especially advertising, as well as sending messages repeatedly on the same site.
b. Spam is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks.

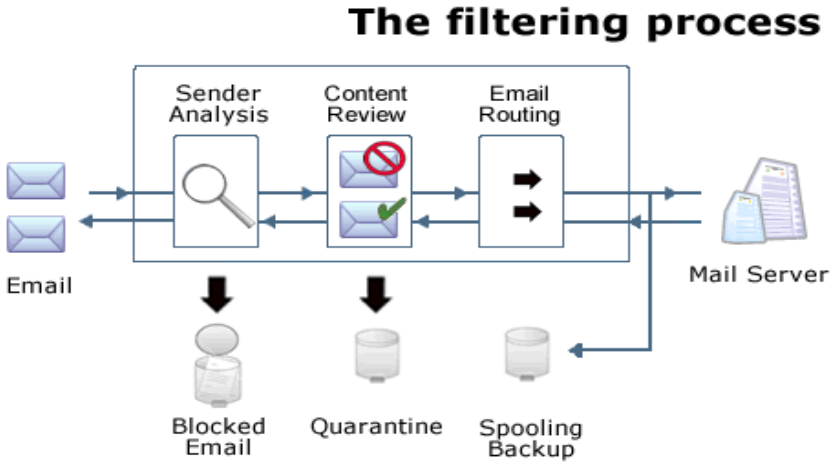


Figure 123: **Filtering process**

20.20 ATTACK PROCESS & TOOLS

a. Spoofing
b. Phishing
c. Hacking
d. Denial of Services
e. Spyware
f. Key logger
g. ATM skimming
h. Password cracking
i. Zombie computer
j. Elevation of Privilege

20.20.1 Spoofing

There are two main types of spoofing

IP spoofing and

E-mail spoofing.

IP spoofing is largely a security exploit—here, the intruder sends data packets that display an IP address different than that of the intruder. Thus, if the packets appear to originate from a computer on the local network, the spoofed IP packet passes through the firewall security without any trouble. This technique is used primarily in one-way attacks such as Denial of Service (DoS) attacks.

20.20.2 Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Mostly carried over on email or IMs This technique, largely used by hackers, fraudulently acquires sensitive information posted on the Internet.

Typically, an attacker sends an e-mail message that seems it has originated from a legitimate Internet address. On occasions, the message includes a hyperlink to websites that seemingly belong to legitimate enterprises. The content on such web pages then request you to verify your personal information or account details. For example, you may receive an e-mail from your bank requesting you to click a hyperlink in the e-mail and verify your online banking information.

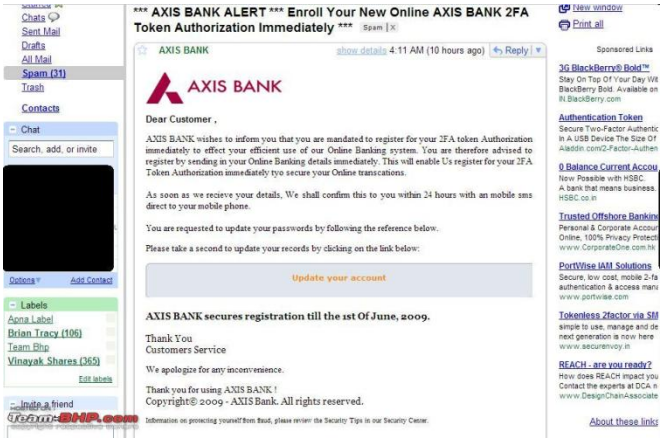


Figure 124: **Phishing**

20.20.3 Hacking

In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls.

Hacking is an unauthorized entry into a network or a computer to steal or manipulate information, data or files. The person involved in this process is named as a hacker. Computer hacking is done using several types of programs such as Rootkit, Trojan, Key logger etc. Hackers also employ techniques like browser hijacks, spoofing, phishing etc. to capture user's personal or financial details.

20.20.4 Denial Of Service (DoS)

Intruders launch a Denial of Service (DoS) attack to overload or halt network services such as web or file servers. Such attacks deny authorized access to resources and delay critical operations.

Sometimes a cracker uses a network of zombie computers to sabotage a specific Web site or server. A cracker tells all the computers on his botnet to contact a specific server or Web site repeatedly. The sudden increase in traffic can cause the site to load very slowly for legitimate users. Sometimes the traffic is enough to shut the site down completely. We call this kind of an attack a **Distributed Denial of Service (DDoS)** attack

The cracker sends the command to initiate the attack to his **zombie army**. Each computer within the army sends an electronic connection request to an innocent computer called a **reflector**. When the reflector receives the request, it looks like it originates not from the zombies, but from the ultimate victim of the attack. The reflectors send information to the **victim system**, and eventually the system's performance suffers or it shuts down completely as it is inundated with **multiple unsolicited responses** from several computers at once.

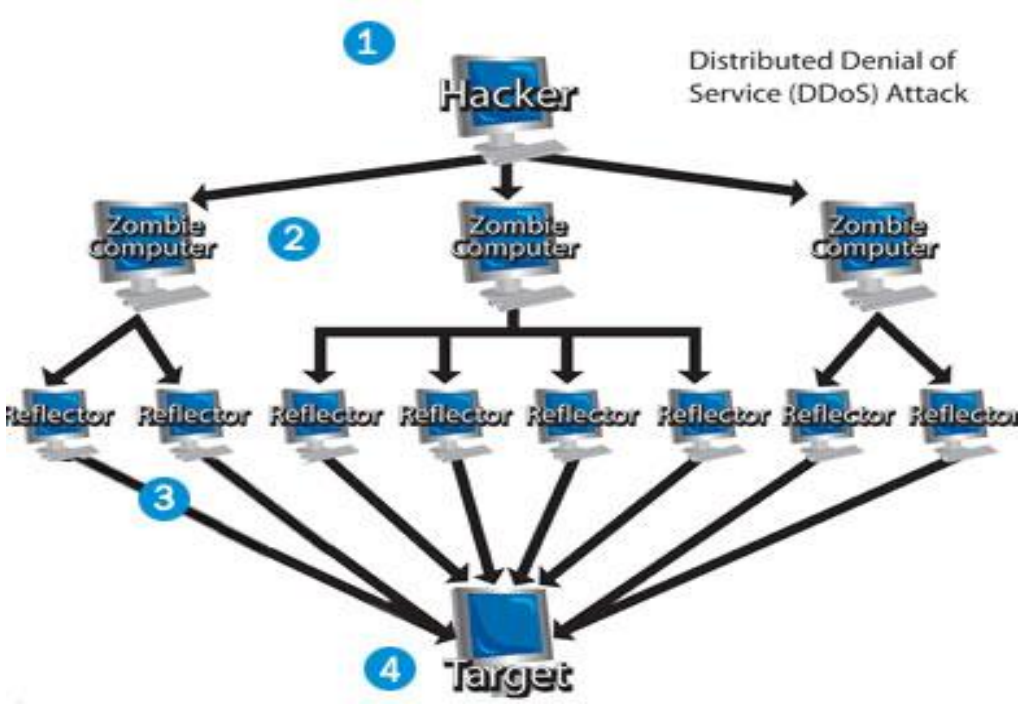


Figure 125: **Denial of Service**

20.20.5 Spyware

A program that covertly gathers information about your online activities without your knowledge is called Spyware. Spyware usually enters the computer while downloading or installing a new program and allows intruders to monitor and access your computer.

Spyware differs from viruses and worms in that it does not usually self-replicate. However, spyware – by design – exploits infected computers for commercial gain. Typical tactics furthering this goal include:

- Delivery of unsolicited pop-up advertisements;
- Theft of personal information (including financial information such as credit card numbers);
- Monitoring of Web-browsing activity for marketing purposes; or
- Routing of HTTP requests to advertising sites.

Figure 126: **Spyware**

20.20.6 Keylogger

Key logger surveillance software has the capability to record keystroke/captures Screen Shots and save it to a log file (usually encrypted) for future use. Captures every key pressed on the computer viewed by the unauthorized user. Key logger software can record instant messages, e-mail and any information you type at any time on your keyboard. The log file created by the key logger can then be saved to a specific location or mailed to the concerned person. The software will also record any e-mail address you use and Website URLs visited by you.

20.20.7 ATM Skimming

It is a technique of compromising the ATM machine by installing a skimming device, at top of the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine.

Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number that are later replicated to carry out fraudulent transaction.

Figure 127: **ATM skimming**

20.20.8 Password Cracking

Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites

20.20.9 Zombie Computer

Refers to a computer that connect to the Internet and is controlled by unauthorized third party without permission and awareness of computer's user. Hacker can use

a. zombie computer in many ways, e.g. Zombies can be used to conduct distributed denial of service attacks or to send spam email.
b. Furthermore hackers have full access to data on a zombie computer, & they can copy, corrupt change or even delete entire of hard copy. Also they can install a software on a zombie computer which help them to get the user name, password, & even financial information of credit card number & bank account to commit fraud.
c. From the perspective of the victim, it looks like the reflectors attacked the system. From the perspective of the reflectors, it seems like the victimized system requested the packets. The zombie computers remain hidden, and even more out of sight is the cracker himself.
d. The list of DDoS attack victims includes some pretty major names. Microsoft suffered an attack from a DDoS called MyDoom. Crackers have targeted other major Internet players like Amazon, CNN, Yahoo and eBay.
e. In e-mail spoofing, the e-mail message is forged so that the true address of the sender is not indicated. Hoax e-mails on security updates bearing a fake Microsoft e-mail address were sent to several e-mail users.
f. Industry leaders, including Microsoft, have now co-developed a technology called the Sender ID Framework (SIDF) to counter e-mail spoofing and

phishing. SIDF validates messages that originate from the mail servers they claim to come from.

20.20.10 Elevation Of Privilege

a. Elevation of privilege is a process by which a user obtains a higher level of privilege than that for which he has been authorized. An intruder may mislead a system into granting unauthorized rights in order to compromise or destroy the system. For example, an attacker might use a guest account to log on to a network, detect a flaw in the software so that the guest privileges can be changed to administrative privileges.

b. "Elevation of privilege," then, is not a class of attack, as much as it is the process of any attack. Virtually all attacks attempt to do something the attacker is not privileged to do. The bad guy wants to somehow leverage whatever limited privilege he has, and turn it into higher ("elevated") privilege.

20.21 DESKTOP SECURITY

A personal computer used without proper security measure could lead to exploiting the system for illegal activities using the resources of such insecure computers. These exploiters could be Virus, Trojans, Key loggers and sometimes real hackers. This may result in data theft, data loss, personal information disclosure, stealing of credentials like passwords etc. So, protect and secure your Personal Computer before it is compromised. The olden phrase is always golden... Prevention is better than Cure

Things to remember while using your personal computer

- Always install Licensed Software so that you have regular updates of your Operating system and Applications. In case of open source software, make sure to update frequently.
- Read the “Terms and Conditions” / “License Agreement” provided by vendor/software before installation.

20.21.1 Guidelines For Desktop Security

Guidelines for Physical

a. Regularly clean your system and its components.
b. Properly organize the power cables, wires, to prevent from water, insects etc.
c. While working at PC, be careful not to spill water or food items on it.
d. Always follow “Safely Remove” option provided by the Operating System while disconnecting the USB devices.
e. By setting BIOS password, you can prevent unauthorized access to your personal computer.

f. Switch of the computer when it's not in use.

20.21.2 Guidelines For Internet Security

Follow Internet Ethics while browsing.

a. Check the copyright issues before using the content of Internet.
b. Always access the site which uses https (Hyper Text Transfer Protocol Secure) while performing online transactions, Downloads etc, which is secure.
c. If the site uses SSL, verify the Certificate details like Who is the owner, Expiry date of the certificate etc to confirm whether it is trusted or not. You can do this by clicking the lock icon.
d. Use only Original Websites for downloading the files rather than Third Party websites.
e. Scan the downloaded files with an updated Anti-Virus Software before using it.
f. Install and properly configure a Software firewall, to protect against malicious traffic.

20.21.3 Guidelines For Data Security

a. Enable Auto-updates of your Operating System and update it regularly.
b. Download Anti-Virus Software from a Trusted Website and Install. Make sure it automatically gets updated with latest virus signatures.
c. Download Anti-Spyware Software from a Trusted Website and Install. Make sure it automatically updates with latest definitions.
d. Use "Encryption" to secure your valuable Information.
e. Note: For encryption password is required, always remember the password used while encrypting it, else data would not be available thereafter.
f. Strong password should be used for "Admin" Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).
g. Backup : Periodically backup your computer data on CD / DVD or USB drive etc.. in case it may get corrupted due to Hard-Disk failures or when reinstalling/format ting the system.

20.21.4 Guidelines For Browser Security

a. Always update your Web Browser with latest patches.
b. Use privacy or security settings which are inbuilt in the browser.
c. Also use content filtering software.
d. Always have Safe Search "ON" in Search Engine.

20.21.5 Guidelines For E-Mail Security

a. Always use strong password for your email account
b. Always use Anti-Spyware Software to scan the e-Mails for Spam.
c. Always scan the e-Mail attachments with latest updated Anti-Virus and Anti-Spyware before opening.
d. Always remember to empty the Spam folder.
e. Startup programs should be monitored / controlled for optimal system performance

20.21.6 Guidelines For Wireless Security

a. Change default Administrator passwords.
b. Turn On WPA (Wi-Fi Protected Access).
c. Change default SSID.
d. Enable MAC address filtering.
e. Turn of your wireless network when not in use.

20.21.7 Guidelines For Modem Security

a. Change the default passwords.
b. Switch of when not in use

20.22 INFORMATION TECHNOLOGY ACT, 2000

By understanding the growing demand and applications of Information Technology, the Government of India passed the bill of Information Technology in 2000, The Information Technology Act, 2000 or ITA, 2000 or IT Act, was notified on **October 17, 2000.** It is the law that deals with cybercrime and electronic commerce in India

The bill was **passed** in the budget session of 2000 and signed by President K. R. Narayanan on **9 June 2000.**

The original Act contained **94 sections**, divided into **13 chapters and 4 schedules**. The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law.

20.22.1 Amendments

A major amendment was made in **2008**. It introduced **Section 66A** which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".

Additionally, it introduced provisions addressing - **pornography, child porn, cyber terrorism and voyeurism**. The amendment was passed on **22 December 2008** without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed into law by President Pratibha Patil, on **5 February 2009**.

The major features of the Act are −

- It facilitates e-governance and e-commerce by providing equal legal treatment to users.
- It made provision to accept electronic records and digital signature.
- It gave legal approval to electronic business transactions.
- The Act instructs banks to maintain electronic record and facilitate electronic fund transfer.
- It also sets up a Cyber Law Appellate Tribunal.

Table 8. List of offences and the corresponding penalties

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹100,000

66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyber terrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to ₹100,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to 2 years, or/and with fine up to ₹100,000

72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to ₹100,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to ₹500,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to ₹100,000
74	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to ₹100,000

20.23 INFORMATION TECHNOLOGY RULES, 2021

The Information Technology (**Intermediary Guidelines and Digital Media Ethics Code**) Rules, 2021 is secondary or subordinate legislation that suppresses India's Intermediary Guidelines Rules 2011. The 2021 rules have stemmed from section 87 of the Information Technology Act, 2000 and are a combination of the draft **Intermediaries Rules, 2018 and the OTT Regulation and Code of Ethics for Digital Media.**

The Central Government of India along with the Ministry of Electronics and Information Technology (MeitY) and the Ministry of Information and Broadcasting (MIB) have coordinated in the development of the rules.

Intermediaries had until 25 May 2021 to comply with the rules.

In the Monsoon session of the Parliament in 2018 a motion on "**Misuse of social media platforms and spreading of fake news**" was admitted. The Minister for Electronics and IT, accordingly made a detailed statement of the "**resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law**". MeitY then prepared the **draft Information Technology (Intermediary Guidelines) Rules 2018 to replace the 2011 rules**. The Information Technology Act, 2000 provided that intermediaries are protected liabilities in some cases. The draft 2018 Rules sought to elaborate the liabilities and responsibilities of the intermediaries in a better way. Further the draft Rules have been made "in order to

prevent spreading of fake news, curb obscene information on the internet, prevent misuse of social-media platforms and to provide security to the users. The move followed a notice issued to WhatsApp in July 2018, warning it against helping to spread fake news and look on as a "**mute spectator**".

20.24 STRUCTURE OF THE INTERMEDIARY RULES

§ Part I of the Intermediary Rules mainly lays down the definitions of terms.

§ Part II deals with the regulation of intermediaries, including social media intermediaries. This part is administered by the Ministry of Electronics and Information Technology or MeitY.

§ Part III deals with the regulation of digital news media (though there is a lack of clarity on exactly which news media these Rules apply to) and OTT platforms. Part III is administered by the Ministry of Information and Broadcasting.

20.25 CONCLUSION

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution.

The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review.

Securing our internet & desktop connection/access not only makes our valuable resources safe from unknown/unauthorized misuse, but also avoids social security related issues. Securing cyber space has a bearing on national security. Unsecured connection is liable to be misused by mischievous persons, anti-social elements and militants.